UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE



Securing America's Digital Future: A Bipartisan Cybersecurity Roadmap for the Next Administration

Recommendations from a Task Force of Leading Cybersecurity Experts

McCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

CSC 2.0

A Report by the McCrary Institute for Cyber and Critical Infrastructure at Auburn University and the Cyberspace Solarium Commission 2.0

Frank J. Cilluffo

RADM Mark Montgomery, USN (Ret.)

George Barnes

Joshua Whitman, PhD

Table of Contents

Table of Contents 2

Executive Summary 4

Unifying the Regulatory Landscape: Coherence for National Security 8

Recommendation 1.1: Conduct a comprehensive review of cybersecurity-related statutes and relevant sector-specific regulations to identify gaps, inconsistencies, and outdated definitions that hinder effective cybersecurity efforts and make recommendations to Congress on addressing them. 9

Recommendation 1.2: While protecting civil liberties and maintaining a balanced approach, synchronize authorities across Titles 10, 18, 32, 33, 40, 44, and 50 to enable more effective coordination between military, intelligence, and law enforcement agencies in cyberspace operations. 10

Recommendation 1.3: Propose legislation to address identified gaps, particularly in areas where existing laws struggle to keep pace with rapidly evolving technology and threats while considering appropriate safe harbor provisions. 10

Recommendation 1.4: Establish a cross-agency task force to streamline and coordinate cybersecurity regulations across agencies/sectors, reducing redundancy and conflicting requirements. 10

Recommendation 1.5: Develop a common set of cybersecurity standards that can be adapted to sector-specific needs while maintaining a baseline level of security across critical infrastructure. 11

Recommendation 1.6: Create a mechanism for regular review and update of cybersecurity and sector-specific security regulations to ensure they remain relevant and effective in the face of evolving threats. 11

Synergy in Cyber Protection: Strengthening National Multi-Stakeholder Collaboration 12

Recommendation 2.1: Rationalize, empower and enhance the role of Sector Risk Management Agencies 14

Recommendation 2.2: Establish a national cybersecurity R&D coordination body 14

Recommendation 2.3: Enhance the Office of the National Cyber Director's role and authorities 14

Recommendation 2.4: Strengthen CISA's capabilities and mandate 14

Recommendation 2.5: Operationalize public-private partnerships 14

Recommendation 2.6: Enhance SLTT cybersecurity capabilities and coordination 15

Recommendation 2.7: Strengthen intelligence sharing and operational coordination 15

Recommendation 2.8: Leverage unique capabilities of key agencies 15

Deterrence and Cost Imposition in Cyberspace: A Strategic Imperative 16

Recommendation 3.1: Strengthen the strategic framework for cyber operations 17

Recommendation 3.2: Enhance operational capabilities through campaign plans and playbooks 17

Recommendation 3.3: Establish a designation process for state sponsors of cybercrime 18

Resilience in Cybersecurity: A Proactive Approach to Risk Reduction 19

Recommendation 4.1: Develop a comprehensive system for critical asset identification and prioritization 20

Recommendation 4.2: Develop comprehensive cloud security and resilience standards and certification processes 20

Recommendation 4.3: Establish sector-specific security standards for IT and OT systems 20

Recommendation 4.4: Strengthen societal resilience against malign cyber influence operations 20

Recommendation 4.5: Examine models for federal government as "Insurer of Last Resort" 21

Cyber Statecraft: Navigating International Cyber Challenges 22

Recommendation 5.1: Strengthen State Department's cyber diplomacy efforts 23

Recommendation 5.2: Promote an open, interoperable internet globally 23

Recommendation 5.3: Enhance international cooperation on cybersecurity standards 23

Building Cyber Capacity: Strategies for a Robust Cybersecurity Workforce 25

Recommendation 6.1: Develop support mechanisms for smaller and rural organizations to access cybersecurity expertise, such as creating virtual CISO organizations 26

Recommendation 6.2: Create a flexible volunteer system that allows cybersecurity professionals to contribute their skills during crises or for specific projects 26

Recommendation 6.3: Implement policies that allow for more flexible employment arrangements, such as part-time government service or short-term assignments for private sector experts 26

Recommendation 6.4: Develop a national K-12 cybersecurity curriculum to build a pipeline of future cyber professionals and cyber literate citizens 26

Recommendation 6.5: Expand existing programs like CyberCorps, Scholarship for Service, and the National Centers of Academic Excellence in Cybersecurity program to cover a wider range of cybersecurity specialties and educational levels 27

Recommendation 6.6: Evolve and expand post-service placement programs to help scholarship recipients transition into key cybersecurity roles in government and critical infrastructure sectors 27

Securing the Future: Safeguarding Critical and Emerging Technologies 28

Recommendation 7.1: Evolve and unify national lists for critical and emerging technologies list and prohibited entities 29

Recommendation 7.2: Enhance supply chain security for critical technologies 29

Recommendation 7.3: Develop a quantum-safe cryptography transition plan 29

Recommendation 7.4: Promote U.S. leadership in key technology areas 30

Foundations of Cyber Resilience: Resources, Economy, and Continuity 31

Recommendation 8.1: Significantly increase budget and resources for Sector Risk Management Agencies 32

Recommendation 8.2: Enhance National Institute of Standards and Technology funding 33

Recommendation 8.3: Resource Cybersecurity and Infrastructure Security Agency and Fund Technology Modernization Funds to Protect Federal Civilian Networks and Critical Infrastructure 33

Recommendation 8.4: Conduct a robust Continuity of the Economy Planning 33

Conclusion 34

Task Force Members 35

Executive Summary

The United States stands at a critical juncture in its cybersecurity journey. As we navigate an increasingly complex and interconnected digital landscape, the challenges we face are not merely technical but existential, threatening the very foundations of our national security, economic prosperity, and democratic way of life. This report, building upon the groundbreaking work of the Cyberspace Solarium Commission[1] while addressing current gaps and emerging threats, presents a comprehensive roadmap for the incoming administration to secure America's digital future.

The scope and severity of cyber threats facing our nation cannot be overstated. In fact, these threats represent an existential threat to our democratic way of life. From state-sponsored attacks and cyber espionage to the relentless surge of ransomware targeting our critical infrastructure, the cyber domain has become a battlefield where our adversaries seek to undermine our strengths and exploit our vulnerabilities.[2] The costs are staggering – hundreds of billions of dollars annually in economic losses are predicted, not to mention the incalculable damage to our national security and the erosion of public trust in our institutions.[3] [4]

Yet, amid these challenges lies an unprecedented opportunity. The incoming administration has the chance to take decisive action, implementing a whole-of-nation approach that harnesses the collective power of government, industry, and individual citizens to secure our digital future. This is not just about defending against threats; it's about positioning the United States to maintain the lead in the growing global digital economy, fostering innovation, and preserving the values that define us as a nation, recognizing that cybersecurity now impacts every aspect of American life – from our economy and national security to our daily personal interactions and democratic processes.

Cybersecurity is inextricably linked to our nation's economic competitiveness on the global stage.[5] It's not just about protecting our assets; it's about maintaining America's technological edge and economic leadership. Strong cybersecurity measures are critical for protecting intellectual property, maintaining business continuity, and fostering innovation. In an increasingly digital global economy, our cybersecurity capabilities directly impact our ability to compete and lead in key industries and emerging technologies.[6] As such, the recommendations in this report should be viewed not only through the lens of national security but as essential components of a comprehensive strategy to enhance America's economic competitiveness.

This report is intended to provide the next administration with a key set of policy recommendations so that they can immediately continue the work of improving the cybersecurity of the United States, amidst growing cyber threats to U.S. critical infrastructure and the lives of everyday Americans. The task force sought to take stock of what is working, what is not working, and what comes next regarding the cyber policy landscape. If adopted, the policy recommendations outlined in this report will demonstrably improve the security and resiliency of U.S. critical infrastructure, and, by extension, the U.S. economy and American way of life. The United States has the opportunity to solidify and expand its role as the preeminent global leader on cybersecurity policy, capabilities, and standards-setting, and it is the objective of this report to provide the incoming administration with the tools necessary to do the job.

This report outlines eight critical themes that demand immediate attention and sustained effort:

1. Harmonization of Cybersecurity Regulation

The current regulatory landscape for cybersecurity is a patchwork of overlapping, sometimes conflicting mandates that often hinder rather than help our security efforts. We must move swiftly to create a coherent, streamlined regulatory framework that enhances security without stifling innovation.

1 Cyberspace Solarium Commission, *Final Report*, March 2020, https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/. For consistency and clarity, this report adopts the definitions established by the Cyberspace Solarium Commission in its final report unless otherwise specified.

2 Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 152-170, https://doi.org/10.1089/elj.2020.0633.

3 Nivedita James Palatty, "90+ Cyber Crime Statistics 2024: Cost, Industries & Trends," *Astra Security Blog*, January 24, 2024, accessed September 22, 2024, https://www.getastra.com/blog/security-audit/cyber-crime-statistics/.

4 Office of Management and Budget, *2024 Report on the Cybersecurity Posture of the United States*, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

5 Chris McCurdy, Shlomi Kramer, Gerald Parham, and Jacob Dencik, *Prosper in the Cyber Economy*, IBM Institute for Business Value, November 14, 2022, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy.

6 Chris McCurdy, Shlomi Kramer, Gerald Parham, and Jacob Dencik, *Prosper in the Cyber Economy*, IBM Institute for Business Value, November 14, 2022, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy.

Key recommendations include:

- Conducting a comprehensive review of cybersecurity-related statutes and regulations to identify gaps and inconsistencies.
- Establishing a cross-agency task force to streamline and coordinate cybersecurity regulations.
- Developing a common set of cybersecurity standards adaptable to sector-specific needs.

The urgency of this task cannot be overstated. Our fragmented regulatory approach is not just inefficient; it's dangerous, creating vulnerabilities that our adversaries are all too eager to exploit.

2. Strengthening Government Coordination

Effective cybersecurity requires seamless coordination across all levels of government and with the private sector.[7] We must break down silos, enhance information sharing, and create mechanisms for rapid, coordinated responses to cyber threats.

Critical recommendations in this area include:

- Enhancing the role and authorities of the Office of the National Cyber Director.
- Strengthening CISA's capabilities and mandate.
- Improving coordination with state, local, tribal, and territorial governments.

3. Cost Imposition and Deterrence

We must move beyond a purely defensive posture to one that imposes real costs on those who would do us harm in cyberspace. This requires a comprehensive strategy that leverages all elements of national power – diplomatic, economic, and, when necessary, military.

Key recommendations include:

- Developing a comprehensive offensive strategy to proactively disrupt and degrade adversary capabilities.
- Establishing a designation process for state sponsors of cybercrime.
- Enhancing our ability to attribute attacks and hold bad actors accountable.

4. Resilience

In an era where cyber attacks are a matter of when, not if, we must build resilience into every aspect of our digital infrastructure. This means not just hardening our defenses but improving our ability to withstand, recover from, and adapt to cyber incidents.

Key recommendations include:

- Developing a comprehensive system for critical asset identification and prioritization.
- Establishing sector-specific security standards for both IT and OT systems.
- Creating a national-level exercise program to test and improve our cyber resilience.

5. Shaping the International Environment

Cybersecurity is a global challenge that requires global solutions. The United States must lead in shaping international norms, standards, and rules of behavior in cyberspace.

Key recommendations include:

- Strengthening the State Department's cyber diplomacy efforts.
- Promoting an open, interoperable Internet globally.
- Enhancing international cooperation on cybersecurity standards.

6. Workforce Development

The shortage of skilled cybersecurity professionals is a critical vulnerability.[8] We must invest in developing a diverse, highly skilled cyber workforce to meet the challenges of today and tomorrow.

Key recommendations include:

- Developing a national K-12 cybersecurity curriculum.
- Expanding programs like CyberCorps and Scholarship for Service.
- Creating flexible volunteer systems and employment arrangements to leverage private sector expertise.

7. Critical and Emerging Technologies

As technologies like artificial intelligence, quantum computing, and 5G reshape our digital landscape, we must ensure that cybersecurity is built into these systems from the ground up.

Key recommendations include:

- Creating a unified national list of critical and emerging technologies.
- Enhancing supply chain security for critical technologies.
- Developing a quantum-safe cryptography transition plan.

7 Office of Management and Budget, *2024 Report on the Cybersecurity Posture of the United States*, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

8 Office of Management and Budget, *2024 Report on the Cybersecurity Posture of the United States*, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

8. Resources, Economy, and Continuity

Effective cybersecurity requires sustained investment and a long-term commitment. We must ensure that our efforts are adequately resourced and aligned with our broader economic and national security goals.

Key recommendations include:

- Significantly increasing budget and resources for Sector Risk Management Agencies.
- Enhancing NIST funding to support its critical work in developing cybersecurity standards.
- Conducting robust Continuity of the Economy planning.

The Imperative of Action

The recommendations outlined in this report are not mere suggestions; they are imperatives for securing America's future in the digital age. The threats we face are real, urgent, and growing more complex by the day. Ransomware attacks, for instance, have moved beyond mere criminal enterprises to become tools of national power, threatening our critical infrastructure and the very fabric of our society.[9] The recent attacks on our healthcare systems, energy grids, and financial institutions are stark reminders of our vulnerabilities and the devastating consequences of inaction.[10]

Yet, the challenge before us is not insurmountable. With decisive leadership, strategic investment, and a whole-of-nation approach, we can not only defend against these threats but position the United States as the global leader in cybersecurity and digital innovation. This is not just about security; it's about maintaining our technological edge, economic competitiveness, and national values in the digital age.

The Path Forward

Implementing the recommendations in this report will require political will, sustained effort, and significant resources. But the cost of inaction far outweighs the investment required. We must:

1. Prioritize cybersecurity as a fundamental pillar of national security and economic policy. This means elevating cybersecurity discussions to the highest levels of government and ensuring that cyber considerations are integrated into all aspects of policy making.
2. Foster a culture of cybersecurity across all sectors of society. From boardrooms to classrooms, we must instill an understanding of cyber risks and best practices.
3. Invest in innovation and research to stay ahead of evolving threats. This includes supporting the development of next-generation cybersecurity technologies and practices.
4. Strengthen public-private partnerships to leverage the full spectrum of our nation's capabilities. The government alone cannot solve this challenge; we need the innovation, agility, and resources of the private sector.
5. Engage internationally to build a coalition of like-minded nations committed to a free, open, and secure cyberspace. Cyber threats know no borders, and our response must be global in scope.

In implementing these measures, we must strike a careful balance between enhancing cybersecurity and protecting individual privacy and civil liberties, ensuring that our efforts to secure cyberspace do not undermine the very values we seek to defend.

Immediate Priorities

While all the recommendations in this report are important, some demand immediate action in the first 100 days of the new administration:

1. Establish a high-level task force to begin the process of regulatory harmonization. This should be a whole-of-government effort, led by the National Cyber Director, with clear deadlines and accountability.
2. Initiate a comprehensive review of our national cybersecurity strategy, with a focus on enhancing our deterrence and cost-imposition capabilities.
3. Launch a national initiative to address the cybersecurity workforce shortage, including immediate steps to expand training programs and create new pathways into the field.
4. Convene a summit of industry leaders to strengthen public-private partnerships and develop concrete plans for enhancing the security of our critical infrastructure.
5. Begin the process of developing a national Continuity of the Economy plan to ensure our ability to maintain essential economic functions in the face of significant cyber disruptions.

These immediate actions are crucial, as there are only a few months to influence the FY27 budget cycle, making it imperative to address major systemic issues promptly.

9 U.S. Government Accountability Office, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support*, GAO-24-106221, January 30, 2024, https://www.gao.gov/products/gao-24-106221.

10 Cybersecurity and Infrastructure Security Agency, "*Stop Ransomware: Official Alerts & Statements*," accessed September 22, 2024, https://www.cisa.gov/stopransomware/official-alerts-statements-cisa/. CISA list of recent attacks.

The Role of Congress

Many of the recommendations in this report will require legislative action. We call on Congress to:

1. Provide the necessary authorities and resources to implement these recommendations fully.
2. Conduct rigorous oversight to ensure effective implementation and accountability.
3. Work in a bipartisan manner to address these critical national security issues.
4. Consider reestablishing an Office of Technology Assessment or similar body to provide Congress with the technical expertise needed to legislate effectively on cyber issues.

A Call to Action

The cyber threats we face are not abstract or distant; they are clear, present, and growing. Every day that passes without decisive action increases our vulnerability and emboldens our adversaries. The incoming administration has a unique opportunity – and a solemn responsibility – to chart a new course in our nation's cybersecurity journey.

This report provides a roadmap, but it will take leadership, commitment, and a shared sense of purpose to turn these recommendations into reality. The stakes could not be higher. Our economic prosperity, national security, and democratic values all hang in the balance.

As we stand at this critical juncture, we must recognize that cybersecurity is not just a technical challenge; it is a fundamental issue of national resilience and global leadership. By taking bold action now, we can secure not just our networks and data, but our future as a nation.

The time for half-measures and incremental steps has passed. We need a paradigm shift in how we approach cybersecurity – one that recognizes its central role in every aspect of our national life. This report calls for nothing less than a mobilization of our national resources and will on a scale not seen since the space race.

But unlike the space race, this is not a competition we can win once and for all. Cybersecurity requires constant vigilance, adaptation, and innovation. It demands a long-term commitment and a fundamental reorientation of how we think about security in the digital age.

The recommendations in this report are ambitious, but they are achievable. More importantly, they are necessary. We cannot afford to wait for the next major cyber attack to spur us to action. The time to act is now.

As we move forward, we must also recognize that cybersecurity is not solely the responsibility of the government. It requires a whole-of-society approach, with every individual, organization, and sector playing their part. From practicing basic cyber hygiene to investing in cutting-edge defenses, we all have a role to play in securing our digital future.

Education and awareness will be critical. We must foster a cybersecurity-conscious culture, where understanding digital risks and responsibilities is as fundamental as any other life skill. This starts in our schools, extends to our workplaces, and must permeate every aspect of our increasingly digital lives.

Moreover, as we strengthen our defenses, we must do so in a way that preserves the openness, innovation, and freedoms that have made the Internet such a powerful force for progress. Cybersecurity should enhance, not constrain, the transformative potential of digital technologies.

International leadership will be crucial. The United States must not only secure its own digital assets but also work to shape a global cyberspace that reflects our values and interests. This means leading by example, fostering international cooperation, and standing firm against those who would use cyberspace for malicious purposes.

The road ahead will not be easy. We will face resistance, setbacks, and new challenges we have yet to anticipate. But the cost of inaction is far greater than the cost of decisive action now. Every day we delay, our adversaries grow stronger, our vulnerabilities deepen, and the task before us becomes more daunting.

But if we act now – with clarity of purpose, unity of effort, and unwavering commitment – we can turn the tide. We can build a digital future that is secure, prosperous, and aligned with our deepest values as a nation. This is the challenge of our time, and this report charts the course to meet it.

In conclusion, this report is not just a set of recommendations; it is a call to action. It challenges us to think bigger, move faster, and commit more deeply to securing our digital future. The incoming administration has a historic opportunity to lead this effort, but success will require the engagement and commitment of every sector of our society.

The choice before us is clear: We can either shape our digital future or be shaped by it. By embracing the recommendations in this report, by marshaling our national will and resources, we can ensure that the United States remains a leader in the digital age – secure, prosperous, and true to our values.

The time for action is now. Our digital future – and with it, the future of our nation – hangs in the balance. Let us meet this moment with the courage, vision, and determination that have defined America's greatest achievements. Together, we can and must secure America's digital future.

01

Unifying the Regulatory Landscape: Coherence for National Security

The United States is facing a critical challenge when it comes to the harmonization of our cybersecurity regulatory frameworks. This challenge goes beyond the desire for bureaucratic streamlining in that it plays a critical role in ensuring the nation's cybersecurity resilience. Further, harmonization will also better promote innovation and help us maintain our global competitive edge. U.S. cybersecurity regulation is a patchwork of laws, regulations, rules, and standards that have evolved incrementally over time in response to specific crises or by addressing more narrow sector-specific needs.[11] This fragmented approach has led to a complex, overly burdensome, and sometimes contradictory regulatory environment that can hinder our collective cybersecurity efforts.[12]

Several factors drive the need for harmonization. First, the nature of cyber threats is inherently cross-sectoral and transnational. A vulnerability in one sector can quickly become a point of exploitation that affects multiple industries and even national security.[13] Second, the rapid pace of technological advancement often outstrips the ability of traditional legislative and regulatory processes to keep up, leading to outdated or ineffective rules.[14] Third, the increasing interconnectedness of our digital infrastructure means that inconsistencies in cybersecurity practices across different sectors or jurisdictions can create systemic vulnerabilities.

One of the primary challenges in the current regulatory landscape is the lack of a comprehensive, up-to-date statutory framework that addresses the full spectrum of cybersecurity issues. Many of our existing laws were written in an era when the internet was in its infancy, and the concept of widespread cyber threats was barely understood. Moreover, some regulations currently applied to cybersecurity were originally intended for other purposes, such as safety or privacy. As a result, these laws and regulations often struggle to address modern cybersecurity challenges effectively.[15] This situation not only calls for harmonization of existing rules but also necessitates a public debate on where new, purpose-built cybersecurity regulations are needed rather than simply extending the scope of outdated laws. For instance, the definition of what constitutes a "U.S. person" in the context of IT systems and data remains ambiguous, creating difficulties in applying laws consistently in our increasingly digital world.

The challenge of harmonization is further complicated by the reality of our interconnected digital world. We live and work in blended ecosystems that combine regulated, non-regulated, and partially regulated technologies, all interacting in complex ways. This interconnectedness demands the effective integration of multiple regulations, standards, and guidelines to ensure comprehensive cybersecurity coverage without gaps. Moreover, while technology is inherently global, regulations remain largely national or regional. Global alignment is primarily achieved through international standards bodies, whose work is then implemented in national-level requirements. This disparity underscores the need to strengthen the linkage between standards and regulations in terms of strategy, focus, and resourcing. Any harmonization effort must, therefore, not only address domestic regulatory inconsistencies but also consider how U.S. regulations align with global standards and practices.

It's important to acknowledge that some agencies, like the Cybersecurity and Infrastructure Security Agency, are responsible for multiple critical infrastructure sectors without having direct regulatory authority. This creates a unique challenge for CISA, which is tasked with coordinating cybersecurity efforts across nine sectors but lacks the regulatory tools to enforce standards or requirements.[16]

This lack of clarity extends to the authorities and responsibilities of various government agencies in cyberspace. The distinctions between military, intelligence, and law enforcement operations in the digital realm are often blurred, leading to potential gaps or overlaps in response capabilities. This situation is further complicated by the fact that cybersecurity threats often require a

11 Office of Management and Budget, *2024 Report on the Cybersecurity Posture of the United States*, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

12 Office of the National Cyber Director, "We Need to Harmonize Cybersecurity Regulations: What We Heard from Our Partners," June 4, 2024, accessed September 22, 2024, https://www.whitehouse.gov/oncd/briefing-room/2024/06/04/we-need-to-harmonize-cybersecurity-regulations-what-we-heard-from-our-partners/.

13 Cybersecurity and Infrastructure Security Agency, "AA22-137A: Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control," May 17, 2022, accessed September 22, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a.

14 Philip Killeen, "U.S. Laws and Mandates Failing the U.S. in the Fast Development of Technology," *Energy Central*, September 18, 2023, accessed September 12, 2024, https://energycentral.com/c/cp/us-laws-and-mandates-failing-us-fast-development-technology/.

15 Jeff Kosseff, "Upgrading Cybersecurity Law," *Houston Law Review* 61, no. 1 (2023): 51-120, https://houstonlawreview.org/article/90792-upgrading-cybersecurity-law.

16 Rebecca Kern, "Cyber Agency Resists Regulator Role as Bills Aim to Expand Power," *Bloomberg Government*, November 10, 2021, accessed September 22, 2024, https://about.bgov.com/news/cyber-agency-resists-regulator-role-as-bills-aim-to-expand-power/.

coordinated response from multiple agencies, each operating under different legal frameworks and constraints.[17]

Additionally, the current regulatory environment significantly burdens organizations, particularly those operating across multiple sectors or jurisdictions. These entities often find themselves navigating a maze of different and sometimes conflicting, cybersecurity requirements. This not only increases compliance costs but can also lead to a focus on meeting specific regulatory requirements rather than addressing the most critical security risks.[18]

The challenges extend beyond our borders. In an interconnected global economy, inconsistencies between U.S. cybersecurity regulations and those of our international partners can create barriers to collaboration and information sharing. This is particularly problematic given the transnational nature of many cyber threats and the need for coordinated international responses.[19]

The recent Supreme Court decision in Loper Bright Enterprises v. Raimondo,[20] which overturned Chevron's deference,[21] has added a new layer of complexity to this harmonization effort. This ruling potentially reduces the ability of regulatory agencies to interpret and implement cybersecurity laws, making it even more crucial for Congress to provide clear, specific guidance in legislation.[22]

In light of this new judicial landscape, there is a growing need for enhanced technical expertise within Congress to craft precise and effective cybersecurity legislation. The lack of an Office of Technology Assessment or a similar entity capable of providing non-partisan, technical analysis to lawmakers is increasingly apparent. Restoring the OTA or establishing a comparable body could significantly aid Congress in understanding complex cybersecurity issues, thereby improving the quality and specificity of cybersecurity laws.[23] This support is crucial in an environment where regulatory agencies' interpretive authority has been curtailed, necessitating more detailed and technically sound legislation from Congress. Such an entity could bridge the gap between rapidly evolving cyber technologies and legislative understanding, ensuring that our laws keep pace with the dynamic cybersecurity landscape.

To address these challenges, we propose a series of recommendations aimed at harmonizing and modernizing our cybersecurity regulatory and statutory framework:

Recommendation 1.1: Conduct a comprehensive review of cybersecurity-related statutes and relevant sector-specific regulations to identify gaps, inconsistencies, and outdated definitions that hinder effective cybersecurity efforts and make recommendations to Congress on addressing them.

This review is crucial for understanding the current state of our cybersecurity laws and identifying areas where they fall short. It should examine not only sector-specific regulations but also overarching laws that impact cybersecurity, such as privacy laws, data protection regulations, and national security statutes. Importantly, this review must include an examination of sector-specific laws and regulations that, while not explicitly designed for cybersecurity, are currently being leveraged or extended to address cyber issues. The review should assess the effectiveness and appropriateness of using these non-cybersecurity-specific regulations to enforce cyber rules, considering the challenges observed in recent implementation efforts.

The review should pay particular attention to definitions and concepts that may have become outdated due to technological advancements. For instance, it should

17 Ines Kagubare, "Portman Warns Against Overlap in Government Cyber Leadership," *The Hill*, August 3, 2022, accessed September 22, 2024, https://thehill.com/policy/cybersecurity/3586868-portman-warns-against-overlap-in-government-cyber-leadership/.

18 Amy Chang, Haiman Wong, and Mumtaz Fatima, *Decoding Organizations' Responses to U.S. Cybersecurity Regulatory Harmonization Efforts with Data Science*, R Street Institute, June 27, 2024, https://www.rstreet.org/research/decoding-organizations-responses-to-u-s-cybersecurity-regulatory-harmonization-efforts-with-data-science/.

19 Maggie Miller, "Could the UN Cybercrime Treaty Be a Russian 'Trojan Horse'?" *Politico*, September 26, 2024, accessed September 22, 2024, https://www.politico.com/news/2024/09/26/un-cybercrime-treaty-white-house-russia-00181271; and Isabella Wilkinson, "What Is the UN Cybercrime Treaty and Why Does It Matter?" *Chatham House*, August 4, 2023, accessed September 22, 2024, https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

20 Loper Bright Enterprises v. Raimondo, 603 U.S. ___ (2024), accessed September 22, 2024, https://www.supremecourt.gov/opinions/22pdf/22-451_7m58.pdf.

21 *Post-Chevron Cyber Regulations with Ari Schwartz & Harley Geiger*, YouTube video, 44:26, posted by McCrary Institute, July 31, 2024, https://www.youtube.com/watch?v=AV0famTgoKM. The US Supreme Court recently overturned Chevron deference, a 40-year-old doctrine that required courts to defer to federal agencies' interpretations of ambiguous laws. This decision empowers judges to independently interpret statutes and potentially overturn agency regulations, making it more challenging for agencies to implement new rules, especially in complex areas like cybersecurity. The ruling has far-reaching implications for regulatory policy across various sectors, potentially leading to more legal challenges against agency actions and increased uncertainty in regulatory landscapes. As a result, both government agencies and private sector entities are now grappling with how to navigate this new legal terrain, particularly in fields where technological advancements often outpace legislative action.

22 Harley Geiger, Ines Jordan-Zoob, and Tanvi Chopra, "Chevron Pattern Disrupted: The Impact on Cybersecurity Regulations," *Center for Cybersecurity Policy and Law*, July 1, 2024, https://www.centerforcybersecuritypolicy.org/insights-and-research/chevron-pattern-disrupted-the-impact-on-cybersecurity-regulations.

23 Darrell M. West, "It Is Time to Restore the US Office of Technology Assessment," *Brookings Institution*, February 10, 2021, accessed September 22, 2024, https://www.brookings.edu/articles/it-is-time-to-restore-the-us-office-of-technology-assessment/.

reconsider how we define critical infrastructure in the digital age, taking into account not just traditional sectors but also emerging critical digital assets and services.[24] This approach will help identify where existing laws are being stretched beyond their original intent.

In light of the Loper Bright decision, this review becomes even more critical as it appears that agencies can no longer rely on broad interpretations of ambiguous statutes. Therefore, the review should focus on identifying areas where statutory language needs to be more precise to withstand potential legal challenges and where new, purpose-built cybersecurity legislation may be necessary.

Recommendation 1.2: While protecting civil liberties and maintaining a balanced approach, synchronize authorities across Titles 10, 18, 32, 33, 40, 44, and 50 to enable more effective coordination between military, intelligence, and law enforcement agencies in cyberspace operations.

The current division of authorities often creates artificial barriers to effective cybersecurity operations. By synchronizing these authorities, we can create a more unified and agile response capability. This synchronization should aim to clarify roles and responsibilities, establish clear chains of command for different types of cyber operations, and create mechanisms for seamless information sharing and coordinated action across agencies. It should also address the unique challenges posed by cyberspace operations that may blur the lines between military, intelligence, and law enforcement activities. The post-Chevron legal landscape makes this synchronization more challenging but also more necessary. Clear delineation of authorities in legislation will be crucial to prevent judicial interpretations that might further fragment the regulatory framework.

Relevant U.S. Code Titles

- Title 10: Armed Forces
- Title 18: Crimes and Criminal Procedure
- Title 32: National Guard
- Title 33: Navigation and Navigable Waters
- Title 40: Public Buildings, Property, and Works
- Title 44: Public Printing and Documents
- Title 50: War and National Defense

Recommendation 1.3: Propose legislation to address identified gaps, particularly in areas where existing laws struggle to keep pace with rapidly evolving technology and threats while considering appropriate safe harbor provisions.

Based on the comprehensive review, new legislation should be proposed to modernize our cybersecurity legal framework. This could include updating key definitions, creating new categories of cyber offenses, establishing clearer jurisdictional boundaries for cyber operations, and providing new tools and authorities for cyber defense and incident response. The legislation should be forward-looking, anticipating future technological developments and creating flexible frameworks that can adapt to emerging threats. Given the new judicial environment, legislation must be more detailed and prescriptive than in the past. Lawmakers should work closely with cybersecurity experts to ensure that statutory language is both technically accurate and legally robust.

This legislative approach should consider incorporating safe harbor provisions that offer legal protections to organizations that implement prescribed cybersecurity standards or best practices. Such provisions can encourage proactive cybersecurity measures by providing clarity on compliance expectations and mitigating concerns about potential liabilities, thereby making new regulations more palatable to the business community while enhancing overall cyber resilience.

Recommendation 1.4: Establish a cross-agency task force to streamline and coordinate cybersecurity regulations across agencies/sectors, reducing redundancy and conflicting requirements.

This task force should bring together representatives from all relevant federal agencies and key industry stakeholders. Building upon existing efforts like Senator Peters' draft legislation[25] and recent congressional testimony,[26] the task force should identify specific areas of regulatory overlap or conflict, pinpointing exact sections of federal code that need harmonization. Its mandate should include proposing solutions for harmonizing requirements, developing mechanisms for ongoing coordination, and aligning cybersecurity regulations with other relevant frameworks, such as privacy regulations and international standards.

This effort should include exploring opportunities for reciprocity of certifications and assessments across requirements for service providers that work with multiple agencies and critical infrastructure sectors, reducing duplicative efforts while maintaining high-security standards.

To address the complex interplay of standards across various domains, the task force should establish a dedicated subgroup focused on aligning multiple cybersecurity standards. This subgroup should consider not only cyber-specific standards but also relevant engineering standards, privacy standards, and others that impact cybersecurity. By addressing the alignment of these diverse standards, the task force can ensure a more comprehensive approach to regulatory harmonization, recognizing that regulating to a standard implicitly requires harmonization of those standards.

24 Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, Time to Designate Space Systems as Critical Infrastructure, Center for Cyber and Homeland Security, April 2023, https://www.fdd.org/wp-content/uploads/2023/04/CSC2.0_Report_Space.pdf. The authors argue, for example, that space infrastructure should be designated as critical infrastructure.

25 Lamar Johnson, "Sen. Peters Drafting Bill for ONCD-Led Cyber Harmonization Panel," MeriTalk, September 13, 2023, accessed September 17, 2024, https://www.meritalk.com/articles/sen-peters-drafting-bill-for-oncd-led-cyber-harmonization-panel/.

26 Nick Leiserson, Testimony before the United States Senate Committee on Homeland Security and Governmental Affairs, June 5, 2024, https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Leiserson-2024-06-05.pdf.

In light of the Loper-Bright decision, the task force must develop strategies to ensure regulatory efforts can withstand increased judicial scrutiny, potentially involving more precise statutory language and additional funding for the judiciary. It should work closely with Congress, possibly exploring the restoration of bodies like the Office of Technology Assessment, to ensure legislators have the necessary technical expertise for effective cybersecurity legislation. The task force should engage with private sector stakeholders to balance enhanced cybersecurity with avoiding undue industry burdens and establish a mechanism for ongoing review and update of the harmonized regulatory framework to address evolving cyber threats and technological advancements.

Recommendation 1.5: Develop a common set of cybersecurity standards that can be adapted to sector-specific needs while maintaining a baseline level of security across critical infrastructure.

While different sectors may have unique cybersecurity needs, a common baseline of security standards can help ensure a minimum level of protection across all critical infrastructure. These standards should be risk-based and outcome-focused, allowing for implementation flexibility while ensuring key security objectives are met. The standards should be developed in close consultation with industry and should leverage existing frameworks where possible, such as NIST's Cybersecurity Framework. In the post-Chevron environment, these standards may need to be more explicitly endorsed or mandated by Congress to ensure their enforceability. The task force should consider recommending legislative action to codify key standards. In addition to focusing on common baselines across different sectors, focused efforts are needed to develop cross-sector mapping[27] among different standards regimes. Cybersecurity is implicated in so many existing standards regimes it is impossible to collapse them all. Consequently, better cross-walking of standards regimes and exploration of mutual recognition agreements are needed to improve the effective implementation of cybersecurity standards.

Recommendation 1.6: Create a mechanism for regular review and update of cybersecurity and sector-specific security regulations to ensure they remain relevant and effective in the face of evolving threats.

Given the rapid pace of technological change and the evolving nature of cyber threats, it's crucial that our regulatory framework remains up-to-date. This mechanism should involve regular assessments of the effectiveness of existing regulations, horizon scanning for emerging threats and technologies, and a streamlined process for updating regulations as needed. It should also include provisions for emergency updates in response to critical new threats or vulnerabilities. This mechanism becomes even more crucial in light of the Loper Bright decision. Regular legislative updates may be necessary to ensure that regulatory frameworks remain effective and legally sound as technology and threats evolve.

Several additional considerations should be kept in mind when implementing the above six recommendations:

First, while harmonization is crucial, it should not come at the expense of sector-specific expertise or the ability to address unique industry challenges. The goal should be to create a coherent overarching framework that can also be further tailored to specific sector needs.

Second, any regulatory harmonization effort should consider international alignment, particularly with key U.S. allies and partners. This could involve exploring ways to create interoperable regulatory frameworks or mutual recognition agreements for cybersecurity standards.

Third, the harmonization process should extend vertically as well as horizontally, addressing inconsistencies between federal, state, and local cybersecurity regulations. This is particularly important for ensuring consistent protection of critical infrastructure that may span multiple jurisdictions.

Fourth, consideration should be given to leveraging existing successful models and exploring how they might be extended or adapted as standards for use in other sectors. This could provide a foundation for creating more unified approaches to areas like cloud security across both public and private sectors.

Finally, while regulatory harmonization is important, it should be balanced with the need for innovation and flexibility. Overly prescriptive regulations can stifle innovation and may quickly become outdated. Therefore, the focus should be on creating a framework that establishes clear security objectives while allowing for flexibility in how those objectives are achieved.

The harmonization of our cybersecurity regulatory and statutory framework is not just a matter of administrative efficiency; it is a strategic imperative for national security and economic competitiveness. By creating a more coherent, up-to-date, and flexible regulatory environment, we can enhance our collective ability to defend against cyber threats, reduce unnecessary compliance burdens, and foster innovation in cybersecurity practices. This harmonization effort will require sustained commitment and collaboration across government agencies, industry sectors, and international partners, but the benefits in terms of improved security, reduced costs, and enhanced resilience make it a critical priority for the incoming administration.

27 Idaho National Laboratory, "Energy Sector Cybersecurity Standards and Best Practices," accessed September 22, 2024, https://energyicsstandards.inl.gov/. An example of cross-sector mapping cybersecurity standards for the energy sector.

02 Synergy in Cyber Protection: Strengthening National Multi-Stakeholder Collaboration

The need for robust coordination across various stakeholders in cybersecurity has never been more critical. The complex nature of cyber threats demands a cohesive and efficient approach to incident prevention and response. This section explores the imperative of enhancing multi-stakeholder coordination, addressing the intricate web of relationships between federal agencies, state, local, tribal, and territorial entities, and the private sector.

While evolving, the current cybersecurity ecosystem often suffers from fragmentation and duplication of efforts. This inefficiency hampers effective response to cyber incidents and leaves vulnerabilities that malicious actors can exploit. By strengthening coordination, we can create a more resilient and responsive cybersecurity posture for the nation.

Operational collaboration among key agencies such as the FBI, DHS/CISA, DOD, and NSA forms the backbone of our national cybersecurity efforts. These agencies bring unique capabilities and perspectives to the table. With its domestic intelligence and law enforcement mandate, the FBI plays a crucial role in cybercrime investigations and threat response. The NSA, leveraging its foreign intelligence capabilities, provides invaluable insights into international cyber threats. The DoD contributes its vast resources and expertise in defending against nation-state actors and sophisticated cyberspace operations.

However, due to coordination challenges and resource constraints, these agencies' full potential remains unmet.[28] Scaling up the FBI's activities in cost imposition strategies and enhancing the NSA's role in bringing intelligence to bear on cyber threats are critical steps. These agencies possess collection capabilities that, when properly leveraged and coordinated, can significantly bolster our cyber defenses.

The NSA's Cybersecurity Collaboration Center, for instance, represents a significant step forward in operational collaboration. By bringing together government and industry partners, it facilitates the sharing of critical cybersecurity information and enhances our collective ability to defend against sophisticated cyber threats. The center's focus on analyzing and disseminating information about nation-state actors and their tools provides invaluable intelligence to both government and private sector entities.

Moreover, the United States Secret Service, often overlooked in cybersecurity discussions, brings unique capabilities to the table, particularly in financial crimes and critical infrastructure protection. Incorporating the USSS more prominently into our coordinated cybersecurity efforts can enhance our overall defensive posture. Their expertise in investigating complex financial crimes, coupled with their role in protecting critical infrastructure, makes them a valuable asset in the fight against cyber threats.

A key aspect of strengthening coordination lies in prioritizing the needs of critical infrastructure owners and operators. These entities form the backbone of our national security and economic well-being. Effective coordination between government agencies and critical infrastructure operators is essential for rapid threat information sharing, incident response, and resilience planning. The growing focus on operational technology in critical infrastructure sectors further highlights the need for specialized knowledge and tailored coordination mechanisms.

The role of Sector Risk Management Agencies cannot be overstated in this context. SRMAs serve as the primary federal interlocutors for their respective critical infrastructure sectors, bridging the gap between government and industry. However, their effectiveness has been hampered by resource constraints and unclear delineations of responsibility.[29] Empowering SRMAs with adequate resources, expected baseline capabilities, and clear mandates is crucial for improving sector-specific cybersecurity coordination.

It's important to note that CISA, as the national coordinator for critical infrastructure security and resilience, plays a crucial role in drawing up and maintaining lists of critical assets and entities across multiple sectors despite lacking direct regulatory authority in many of these areas.

Another crucial element in the coordination landscape is the Office of the National Cyber Director. Established to provide strategic direction and oversight of national cybersecurity policy and strategy, ONCD's role in facilitating interagency coordination and public-private partnerships is pivotal. However, to fulfill its mandate effectively, ONCD requires enhanced authorities and resources. The office's potential to serve as a central coordinating body for national cybersecurity efforts is significant, but it needs to be fully realized through a clear delineation of responsibilities – clarifying the roles of the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency (CISA) serving within the Department of Homeland Security, the federal Chief Information Security Officer now serving within the Office of Management and Budget and informally

28 U.S. Government Accountability Office, *Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767, September 2022, https://www.gao.gov/assets/d22104767.pdf.

29 U.S. Government Accountability Office, *Critical Infrastructure Protection: Time Frames to Complete CISA Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-106720, March 23, 2023, https://www.gao.gov/assets/gao-23-106720.pdf.

dual-hatted as the Deputy NCD for federal cyber security, and National Security Council - and robust support from other federal entities (see also recommendation 2.3).

The Cybersecurity and Infrastructure Security Agency, as the nation's risk advisor, plays a central role in coordinating cybersecurity efforts across the civilian federal government and with the private sector.[30] Strengthening CISA's capabilities and clarifying its responsibilities vis-à-vis other agencies is crucial for a more coherent national cybersecurity strategy. CISA's role in information sharing, threat analysis, and incident response coordination positions it as a key player in the national cybersecurity ecosystem. However, challenges remain in terms of its authority to compel action from other federal agencies, its ability to streamline and/or integrate the federal government's engagement of the private sector, and its own capacity given longstanding resource limitations to engage effectively with the private sector.[31]

The Cyber Safety Review Board has emerged as a best practice in fostering accountability and driving improvements in cybersecurity. Their comprehensive reports have prompted significant response actions from both government and industry stakeholders. The CSRB's model of in-depth incident analysis and actionable recommendations should be highlighted and potentially expanded to cover a wider range of significant cyber incidents.

The importance of operational models that bring together government and private sector entities cannot be overstated. Initiatives like the Joint Cyber Defense Collaborative,[32] the NSA's Cybersecurity Collaboration Center,[33] and Project Fortress[34] in the financial sector demonstrate the power of operationalized public-private partnerships. Expanding and replicating these models can significantly enhance our collective cyber defense capabilities. These collaborative efforts improve information sharing and foster a deeper understanding of the threat landscape while promoting the development of joint strategies to address cybersecurity challenges.

The U.S. Cyber Command's Cyber National Mission Force[35] plays a crucial operational role in thwarting foreign malicious cyber activity threats and actions against U.S. interests. The CNMF works closely with the National Security Agency to gather intelligence and with the Federal Bureau of Investigation to take action. This collaborative approach exemplifies the kind of interagency cooperation necessary to effectively combat sophisticated cyber threats. Strengthening the CNMF's capabilities and enhancing its integration with other key cybersecurity entities should be a priority in our national cyber defense strategy.

The concept of co-managed risk and resilience organizations, drawing inspiration from models like the North American Electric Reliability Corporation, offers a promising avenue for enhancing public-private collaboration. Such organizations can provide a structured framework for sharing information, developing standards, and coordinating response efforts across critical infrastructure sectors. These organizations can help bridge the gap between public and private sector cybersecurity efforts by involving both government and private sector stakeholders in governance and decision-making processes.

The role of state, local, tribal, and territorial entities in national cybersecurity efforts is often underappreciated. These entities are often on the front lines of cyber incidents, particularly those affecting critical infrastructure and essential services at the local level. Enhancing the cybersecurity capabilities of SLTT governments and improving their coordination with federal efforts is crucial for building a comprehensive national cybersecurity posture. This includes not only providing resources and training but also ensuring that SLTT entities are integrated into national-level cybersecurity planning and exercises.

The National Guard plays a unique role in bridging the gap between federal and state-level cybersecurity efforts. With its dual state-federal mission, the National Guard can provide critical cyber capabilities to support both state and federal responses to cyber incidents. Leveraging the National Guard's cyber units more effectively in national cybersecurity efforts could significantly enhance our overall resilience and response capabilities.

Research and development in cybersecurity is another area where improved coordination can yield significant benefits. Currently, cybersecurity R&D efforts are often fragmented across various government agencies, quasi-government entities, academic institutions, and private sector entities. Establishing a national-level coordination body for cybersecurity R&D could help align research priorities with national needs, identify gaps, reduce duplication of efforts, and accelerate the transition of research findings into practical applications.

30 The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

31 U.S. Department of Homeland Security, *CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation*, Office of Inspector General, March 2023, https://www.oig.dhs.gov/sites/default/files/assets/2023-03/OIG-23-19-Mar23.pdf.

32 Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," accessed September 22, 2024, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.

33 National Security Agency, "Cybersecurity Collaboration Center," accessed September 22, 2024, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.

34 "Treasury Department Launches Cybersecurity Initiative for Financial Services," *ABA Banking Journal*, May 9, 2024, accessed September 11, 2024, https://bankingjournal.aba.com/2024/05/treasury-department-launches-cybersecurity-initiative-for-financial-services/.

35 U.S. Cyber Command, "About the Cyber National Mission Forces," accessed September 22, 2024, https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/.

In light of these considerations, we propose the following recommendations to strengthen coordination in the cybersecurity domain:

Recommendation 2.1: Rationalize, empower, and enhance the role of Sector Risk Management Agencies

Strengthen the roles and responsibilities of SRMAs, emphasizing their unique position in coordinating sector-specific cybersecurity efforts. Enhance coordination mechanisms between SRMAs and other agencies like CISA to avoid duplication of efforts and ensure seamless collaboration. Rationalize the number of sectors where CISA serves as SRMA and the Agency's approach to do so to ensure that the SRMA role is separated from the National Coordinator one. Establish clear lines of accountability within SRMAs, ensuring that those with decision-making authority also have the ability to influence resource allocation and implementation of cybersecurity measures. Develop clear metrics and performance indicators to assess the effectiveness of SRMAs in improving their sectors' cybersecurity posture. Additionally, a comprehensive review of critical infrastructure designations and SRMA assignments should be conducted, assessing whether emerging sectors, such as the space sector, should be independently considered under NSM-22[36] due to their growing importance in national security and the economy. This review should also evaluate SRMA assignments and the need for new SRMAs to address evolving technological landscapes and emerging threats. NSM-22 maintained a sector structure that is likely outdated and missed an opportunity to better harmonize with NATO allies. The sector structure should be freshly evaluated based on a set of defined and transparent criteria to capture the cyber risk environment.

Furthermore, as part of this comprehensive review, consideration should be given to expanding the definition of critical infrastructure sectors in NSM-22 to include space infrastructure.[37] The increasing reliance on space-based assets for communication, navigation, and other critical functions underscores the need to recognize and protect space infrastructure as a vital component of national security and economic stability. Adding space infrastructure to NSM-22 would ensure that this crucial sector receives the necessary attention, resources, and protection commensurate with its importance to national interests.

Recommendation 2.2: Establish a national cybersecurity R&D coordination body

The National Science and Technology Council[38] coordinates R&D efforts among federal agencies. Building on existing work within NSTC and the Office of Science and Technology Policy in the White House, further efforts are needed to coordinate cyber-related R&D specifically, as it applies to so many critical and emerging technologies. Additionally, greater nationally-focused coordination on cyber R&D is needed. Thus, we recommend creating a national-level coordination mechanism for cybersecurity research and development efforts across government agencies, industry, and academia. This mechanism, developed within the National Security Council process, will ensure inclusive private sector input while minimizing duplication of efforts, maximizing impact, and aligning research priorities with national cybersecurity needs. It will facilitate the sharing of research findings, promote collaborative projects, and help bridge the gap between theoretical research and practical application in cybersecurity. By involving both public and private stakeholders, this approach will ensure that R&D efforts are responsive to real-world challenges and opportunities in the cybersecurity landscape.

Recommendation 2.3: Enhance the Office of the National Cyber Director's role and authorities

Establish ONCD as the primary coordinator for cyber incident response, bringing together inputs from agencies like NSA, DoD, CISA, SRMAs, and FBI during major cyber incidents. Empower ONCD with additional authorities to drive interagency coordination, including the ability to influence budget allocations for cybersecurity initiatives across agencies. Implement ONCD-led integrated portfolio reviews to assess and coordinate cybersecurity investments across the federal government, ensuring the involvement of the Office of Management and Budget. Create a formal mechanism for ONCD to engage with and coordinate efforts of SRMAs, fostering a more cohesive approach to sector-specific cybersecurity challenges.

Recommendation 2.4: Strengthen CISA's capabilities and mandate

Provide adequate funding for CISA's operational systems and managed services offerings for federal agencies. Clarify CISA's roles and responsibilities to avoid duplication with other agencies while ensuring it has the necessary authorities, resources, and staffing required for its mission. Enhance CISA's ability to coordinate with state, local, and private sector entities, not just federal agencies. Enhance CISA's ability to partner more effectively with other agencies, including DoD, the Intelligence Community, and independent regulators, to improve coordination and collaboration on cybersecurity efforts.

Recommendation 2.5: Operationalize public-private partnerships

Establish co-managed risk and resilience organizations, drawing inspiration from the NERC model of the 1960s, to enhance public-private collaboration. Develop a secure, real-time information-sharing platform to rapidly disseminate actionable threat intelligence between government and critical infrastructure operators. Integrate private sector companies more effectively into coordinated cyber incident response efforts. Establish, expand, and

36 The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024, accessed September 22, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

37 Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, Time to Designate Space Systems as Critical Infrastructure, Center for Cyber and Homeland Security, April 2023, https://www.fdd.org/wp-content/uploads/2023/04/CSC2.0_Report_Space.pdf. The authors argue, for example, that space infrastructure should be designated as critical infrastructure.

38 The White House, "National Science and Technology Council," accessed September 22, 2024, https://www.whitehouse.gov/ostp/ostps-teams/nstc/.

improve the operational models similar to JCDC, ETAC, Project Fortress, Europol, NCIJTF, JTTF, and NSA's Cybersecurity Collaboration Center that bring together government and private sector entities for joint cyberspace operations and threat response. Consider creating a private sector analogue to the NCIJTF for coordinating disruption activities against cyber threats. Additionally, it should be considered that NCIJTF currently lacks resources to accomplish its role comanaging cyber incident response. If the goal is to continue leveraging NCIJTF going forward, it will likely require additional resources to be effective.

Recommendation 2.6: Enhance SLTT cybersecurity capabilities and coordination

Enhance and expand the existing grant program to better support SLTT governments in strengthening their cybersecurity capabilities and aligning them with federal standards and practices. Increase funding and improve utilization of these resources to maximize their impact across state, local, tribal, and territorial entities. Implement a comprehensive National Cyber Resilience Exercise Program that regularly tests and improves coordination between federal and SLTT entities in responding to cyber incidents. Consider leveraging existing structures such as fusion centers to enhance cyber threat information sharing and coordination at the SLTT level. This effort should include regular national-level exercises involving federal, state, local, tribal, and territorial entities, integrate National Guard cyber capabilities, use diverse scenarios including tabletop exercises, emphasize improving real-time coordination and resource allocation during crises, and involve private sector partners to enhance public-private coordination. Leverage and expand successful training models such as the National Computer Forensics Institute, which provides crucial cybersecurity training for law enforcement and serves as an exemplar for developing cyber skills across various sectors. Current, periodic exercising is insufficient in generating the depth of trust needed among critical stakeholders at varying levels of government, and consideration should be afforded to how engagements can become more frequent and direct points of contact for incident management can be made.

Recommendation 2.7: Strengthen intelligence sharing and operational coordination

Enhance mechanisms for sharing classified threat intelligence with cleared private sector leaders, particularly those in critical infrastructure sectors. Implement a reform for cyber positions across the government, requiring interagency experience for career advancement in cybersecurity roles akin to the Goldwater-Nichols Act. This will foster a more integrated and coordinated approach to cybersecurity across different agencies. Develop clear processes and focused resourcing for rapid downgrading, declassification, and sharing of actionable threat intelligence during cyber incidents. This should include mechanisms for downgrading classified intelligence to the For Official Use Only level for controlled sharing with pertinent entities, as well as full declassification when appropriate. It's crucial to establish efficient procedures for both processes, recognizing that downgraded information remains controlled while declassified information has all controls removed. Any review should determine if legislative changes are required to facilitate improved intelligence sharing and operational collaboration. This nuanced approach will enable more timely and appropriate sharing of critical threat intelligence with relevant stakeholders while maintaining necessary protections for sensitive information.

Recommendation 2.8: Leverage unique capabilities of key agencies

Scale up FBI's activities in cost imposition strategies against cyber adversaries, focusing on disrupting cybercriminal ecosystems and deterring state-sponsored cyber activities. Enhance FBI's technical capability through appropriations to allow it to better scale and conduct global on-network infrastructure disruptions. Enhance the NSA's role in providing actionable foreign intelligence to support both government and private sector cybersecurity efforts. This enhancement should include a careful review and potential expansion of NSA's current authorities, which currently constrain operational collaboration with industry beyond the Defense Industrial Base and DIB-supporting entities. While maintaining necessary safeguards, consider broadening the NSA's ability to engage directly with a wider range of critical infrastructure sectors in partnership with SRMAs, balancing improved threat intelligence sharing with appropriate privacy protections and oversight mechanisms. Expand the USSS's involvement in cybersecurity efforts, particularly in areas related to financial crimes and critical infrastructure protection.

The challenges we face in cyberspace are complex and ever-evolving. No single entity – government or private – can address these challenges alone. It is only through robust, well-coordinated efforts that we can hope to stay ahead of adversaries and protect our national interests in the digital age. As we move forward, we must remain committed to fostering a culture of collaboration, information sharing, and mutual support across all sectors involved in our nation's cybersecurity.

The path to enhanced coordination is not without obstacles. It requires overcoming institutional inertia, bridging cultural divides between different sectors, and navigating complex legal and policy frameworks. However, the potential benefits – a more secure digital infrastructure, improved resilience against cyber threats, and a stronger national security posture – far outweigh the challenges. By committing to these recommendations and fostering a truly collaborative approach to cybersecurity, we can build a safer, more secure digital future for all Americans.

03 Deterrence and Cost Imposition in Cyberspace: A Strategic Imperative

The United States faces an unprecedented challenge in the cyber domain: how to effectively deter and impose costs on adversaries who operate with relative impunity in the digital domain. The traditional models of deterrence, rooted in Cold War-era strategies, require significant adaptation to address the unique characteristics of cyberspace. This section builds upon and extends the framing of deterrence in the cyber environment as established by the Cyberspace Solarium Commission, emphasizing the need for a more proactive and assertive approach.

The "dissuade, deter, compel" model provides a useful framework for understanding cyber deterrence. In this context, dissuasion aims to prevent adversaries from developing or expanding their cyber threat capabilities. Deterrence seeks to convince potential attackers that the costs of their actions will outweigh any perceived benefits. Compellence, the most assertive stance, involves forcing an adversary to change their behavior through the threat or use of punitive measures.

The challenges of attribution and escalation management in cyberspace significantly influence the development and implementation of effective deterrence strategies. Unlike conventional warfare, cyber attacks often occur below the threshold of armed conflict, making it difficult to justify traditional military responses. Moreover, the ability to definitively attribute attacks to specific actors remains a persistent challenge, complicating efforts to hold adversaries accountable.

The exponential rise of cybercrime demands an escalated international response.[39] Ransomware attacks alone are projected to cost the world more than $40 billion in 2024,[40] affecting nation-states, major corporations, critical infrastructure providers, schools, hospitals, and ordinary citizens. This challenge is exacerbated by the proliferation of cybercrime safe havens – nations that allow cybercriminal syndicates to operate within their borders without fear of extradition or prosecution. These safe havens provide cybercriminals with the stability and infrastructure to plan complex attacks and safely store illicit proceeds, further complicating efforts to attribute and respond to cyber threats.

To address these challenges, the United States must recalibrate its escalation-risk calculus, demonstrating a willingness to take more offensive deterrent actions against cyber threats. This shift requires a delicate balance – maintaining a robust defensive posture while developing and deploying offensive capabilities that can precisely target adversary systems with minimal collateral damage.

The concept of "defend forward" represents a strategic approach that aligns with this more assertive stance. This approach must be balanced with robust defensive measures and enhanced international cooperation to ensure a comprehensive and effective cyber deterrence strategy. By proactively disrupting and degrading adversary cyber capabilities before they can be used against U.S. interests, this strategy aims to shape the behavior of potential attackers and raise the costs of malicious cyber activities.

However, the implementation of such strategies must be carefully calibrated. The evolving nature of cyber threats necessitates flexible, adaptable deterrence mechanisms that can respond to a range of potential scenarios. Furthermore, any offensive actions must be weighed against the risk of escalation and potential impacts on international relations.

These additional costs span multiple domains, each designed to increase the financial, operational, and reputational burdens on malicious actors. Financial costs can be imposed through targeted sanctions on individuals, organizations, and state-sponsored entities involved in cybercrime, including asset freezes and restrictions on access to international financial systems. Operational costs can be inflicted by disrupting the infrastructure used by cybercriminals, such as command and control servers and communication channels, forcing adversaries to expend more resources to maintain their operations. Technical costs can be increased through the development and deployment of advanced defensive technologies, making attacks more difficult and time-consuming to execute.

Intelligence costs can be raised by enhancing information sharing among allies and partners, increasing the risk of exposure for adversaries. Reputational costs can be imposed through strategic communication campaigns that publicly attribute attacks to specific actors, damaging their credibility and hampering their ability to recruit talent or form alliances. Diplomatic costs can be leveraged by isolating bad actors in international forums, restricting their engagement in legitimate international commerce and diplomacy. Legal costs can be pursued through civil litigation against cyber criminals and their enablers, potentially seizing assets and disrupting their business models. Finally, market costs can be imposed by working with private sector partners to make

39 U.S. Department of Justice, *Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks*, September 2024, https://oig.justice.gov/sites/default/files/reports/24-107.pdf.

40 Cybersecurity Ventures, "Cybercrime to Cost the World $9.5 Trillion USD Annually in 2024," eSentire, 2023, accessed September 22, 2024, https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024.

certain types of attacks economically unviable, such as coordinating ransom payment policies to reduce the profitability of ransomware attacks.

Implementing this broader approach requires a whole-of-government effort, leveraging diplomatic, economic, and intelligence tools in addition to law enforcement and military capabilities. The development of a clear, consistent strategy for imposing costs on adversaries in cyberspace is essential to shape their behavior and protect U.S. interests in the digital domain. This multifaceted approach recognizes that adversaries in the interconnected digital landscape must simultaneously be confronted on multiple fronts to effectively deter malicious activities and safeguard national security.

A critical aspect of effective deterrence and cost imposition in cyberspace is the ability to trace and disrupt the financial flows that sustain cybercriminal operations. However, today's efforts to 'follow the money' as a key component of ransomware actor attribution and cost imposition are significantly hindered by robust obfuscation capabilities employed by malicious actors. This challenge affects intelligence gathering, law enforcement actions, and other cost-imposition operations. Enhancing our capabilities to illuminate these obfuscated finance flows is crucial for undermining the economic incentives driving cybercrime and for improving our ability to attribute attacks to specific actors or groups. Investment in advanced technologies and methodologies to track complex financial trails will be essential in strengthening our overall deterrence and cost imposition strategies.

With these considerations in mind, we propose the following recommendations to enhance the United States' ability to impose costs and deter malicious cyber activities:

Recommendation 3.1: Strengthen the strategic framework for cyber operations

Maintain and accelerate the legal framework established by National Security Presidential Memorandum 13 for conducting offensive cyber operations while developing a streamlined process for approving time-sensitive cyber operations.[41] This recommendation fully supports the intent of NSPM-13 while seeking to build upon and enhance its framework to meet evolving cyber threats. This recommendation aims to clarify roles, authorities, and processes without delving into classified specifics of NSPM-13. By enabling more effective and timely cyber responses while maintaining appropriate oversight, this approach will enhance the U.S. government's ability to respond to emerging threats.

Furthermore, develop and implement a comprehensive offensive strategy that proactively disrupts and degrades adversary cyber capabilities before they can be used against U.S. interests. This strategy should emphasize a whole-of-government approach, ensuring that all relevant agencies and departments are aligned in their efforts to impose costs on adversaries in cyberspace. This strategy should outline long-term approaches for imposing costs and shaping adversary behavior, while also establishing clear guidelines for escalation management and international cooperation.

Recommendation 3.2: Enhance operational capabilities through campaign plans and playbooks

Under the leadership of CISA, consistent with Section 1715 of the FY21 NDAA, developed detailed, adaptable playbooks for responding to various types of cyber incidents and adversary actions, reducing response time and ensuring consistency across government agencies. This effort should be coordinated through the normal interagency National Security Council-led process to ensure comprehensive input and alignment. These playbooks should be complemented by the creation of campaign plans for persistent engagement with specific adversaries, outlining both short-term and long-term strategies for imposing costs and shaping behavior.

Establish a regular review and update process for these plans and playbooks to ensure they remain relevant and effective in the face of evolving cyber threats. Conduct regular exercises to test and refine these plans, involving both government agencies and private sector partners as appropriate. This collaborative approach will help build a more resilient and responsive cyber ecosystem.

Develop metrics to assess the effectiveness of cyber deterrence activities and inform strategic decision-making. This framework should include methods for assessing and measuring the effectiveness of non-traditional cost imposition tactics, broadening our understanding of successful cyber deterrence beyond traditional metrics like arrests and prosecutions. These metrics should be integrated into the playbooks and campaign plans, providing a framework for evaluating the success of deterrence efforts and guiding future strategy development.

Invest in the development of advanced cyber capabilities that can precisely target adversary systems while minimizing collateral damage. These capabilities should be aligned with the strategic objectives outlined in the campaign plans and playbooks, ensuring that the United States maintains a technological edge in the cyber domain.

Developing attribution standards and mechanisms for sharing intelligence and technical analysis related to cyber incidents with allies and partners is another crucial aspect of this recommendation. By establishing common frameworks and protocols for attributing cyber attacks and sharing

41 Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," C4ISRNet, May 8, 2019, accessed September 22, 2024, https://www.c4isrnet.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.

related information, the U.S. can enhance collective defense capabilities and improve the global community's ability to hold malicious actors accountable.

Recommendation 3.3: Establish a designation process for state sponsors of cybercrime

Create a formal process for designating nations as state sponsors of cyber attacks, similar to the existing state sponsors of terrorism list.[42] This designation process should explicitly address the issue of nations providing safe haven to cybercriminal groups, recognizing that allowing cybercriminals to operate freely within a nation's borders is tantamount to state sponsorship of cyber attacks. This process should address both direct cyber attacks and the provision of safe haven to cybercriminal groups, recognizing the symbiotic relationships that often exist between state actors and cybercriminal organizations. This approach aligns with recent legislative efforts, such as Sen. Mark Warner's proposal to treat ransomware threats with the same level of priority as terrorism, highlighting the growing recognition of cyber threats as national security issues.[43]

Russia and North Korea exemplify the model of state cyber sanctuaries. Despite public condemnations, these nations quietly support hacking groups, with cybercriminals sharing stolen data with state intelligence agencies in exchange for refuge from U.S. law and access to money laundering services. North Korea has even institutionalized cybercrime to circumvent international sanctions and fund its nuclear program.

Establish clear criteria for such designations, including evidence standards and the types of cyber activities that would qualify. Develop a range of diplomatic, economic, and cyber-specific sanctions that can be applied to designated state sponsors of cyber attacks, ensuring that there are real consequences for nations that engage in or support malicious cyber activities.

This approach should build upon established precedents in combating global threats, such as the State Department's annual reports on global terrorism. Similar annual reports on state-sponsored cybercrime could prove equally effective in identifying major cybercriminal syndicates and documenting their most significant attacks.

Implement a regular review process to assess designated nations and provide a clear path for removal from the list based on changed behavior. This approach incentivizes positive changes in state behavior while maintaining pressure on persistent bad actors.

While some may argue that such designations could escalate tensions between cyber superpowers or that proving explicit state sponsorship sets an unnecessarily high legal bar, these risks pale in comparison to the existential threat that cyber safe havens pose to the rules-based international order. The United States has both the justification and capabilities to productively initiate an international cyber designation regime now, particularly as the constant barrage of cyber attacks collectively poses a significant threat to our security.

By implementing these recommendations, the United States can significantly enhance its ability to impose costs on adversaries in cyberspace and deter future malicious activities. This comprehensive approach, combining strategic vision, operational capabilities, and targeted designations, will position the U.S. to more effectively navigate the complex challenges of the digital age and protect our interests in cyberspace.

42 Frank Cilluffo and Joshua Whitman, "Opinion: This should be America's next step to stay ahead of ruthless cyber criminals," CNN, August 8, 2024, accessed October 11, 2024, https://www.cnn.com/2024/08/08/opinions/state-sponsors-cybercrime-cilluffo-whitman/index.html.

43 Cynthia Brumfield, "Intelligence Bill Would Elevate Ransomware to a Terrorist Threat," CyberScoop, August 6, 2024, accessed September 17, 2024, https://cyberscoop.com/ransomware-terrorism-ndaa-2025/.

04 Resilience in Cybersecurity: A Proactive Approach to Risk Reduction

In the ever-evolving landscape of cyber threats, the concept of resilience has become paramount. No longer is it sufficient to merely withstand attacks; organizations must be prepared to maintain operational continuity and rapidly recover from disruptive cyber incidents.[44] This shift requires a fundamental change in our approach to cybersecurity, moving from a reactive stance to a proactive risk reduction posture.

One of the most pressing issues in this evolving landscape is the identification and protection of our most critical assets. The concept of Systemically Important Entities has emerged as a crucial framework for prioritizing cybersecurity efforts. These are organizations whose compromise could have significant cascading effects on national security, economic stability, or public health and safety. By focusing on SIEs, we can ensure that our most vital assets receive the highest level of protection and support.

However, the challenges extend beyond just identifying critical entities. The increasing reliance on cloud services introduces new vulnerabilities that must be addressed. Cloud environments present unique security challenges, including multi-tenancy risks and supply chain vulnerabilities. Establishing comprehensive standards and certification processes for cloud security and resilience, particularly for critical infrastructure and SIEs, is essential to mitigate these risks.[45]

While cloud environments present unique security challenges, they also offer significant security advantages. Cloud service providers often have more robust security measures, regular updates, and dedicated security teams that can enhance an organization's overall security posture. The scalability and flexibility of cloud services also allow for more rapid response to emerging threats.

The convergence of information technology and operational technology systems presents both opportunities and challenges. Physical systems are increasingly digitized, censored, and interconnected. As the lines between these domains blur, organizations face unprecedented complexity in safeguarding their digital assets, an increasing volume of data, and critical infrastructure. This convergence necessitates a comprehensive strategy that addresses both the technological and operational aspects of cybersecurity.

The distinct nature of OT systems requires special consideration and recognition of the specialized needs for securing these systems. Traditional IT security approaches may not be sufficient or appropriate for OT environments, which often involve legacy systems and have different operational requirements. Developing sector-specific security standards aligned to other non-cyber standards prevalent in OT system requirements, and that address both IT and OT systems is crucial to ensure comprehensive protection across all critical infrastructure sectors.

The cybersecurity landscape is further complicated by the rapid growth of technology startups, which often develop critical components or services used across various sectors. Recent incidents, such as the SolarWinds breach, highlight the potential for supply chain vulnerabilities originating from these younger companies.[46] Startups, while driving innovation, may lack the resources or experience to implement robust cybersecurity measures, especially in their early stages. This gap presents a twofold challenge: ensuring that startups adhere to appropriate cybersecurity standards and safeguarding the investment processes in these companies to prevent potential exploitation by foreign adversaries seeking access to emerging technologies. Addressing these challenges requires a delicate balance between fostering innovation and maintaining security, potentially through tailored cybersecurity guidelines for startups and enhanced scrutiny of early-stage investments in critical technology areas.

As we strengthen our technological defenses, we must not overlook the human element of cybersecurity. Malign cyber influence operations pose a significant threat to societal resilience, if not to the foundational elements of Democracy. These operations, often orchestrated by foreign actors, aim to manipulate public opinion, sow discord, and undermine trust in institutions. Countering these threats requires a multifaceted approach that combines law enforcement efforts, proactive engagement strategies, and public awareness initiatives.

Finally, as the scale and sophistication of cyber threats continue to grow, we must consider innovative approaches to risk management. The concept of the federal government serving as an "insurer of last resort" for catastrophic cyber events merits serious examination. Such a model, similar to the TRIA

44 Marsh McLennan and Zurich Insurance Group, *Closing the Cyber Risk Protection Gap*, September 2024, https://www.marshmclennan.com/assets/insights/publications/2024/september/mmc-zurich-cyber-whitepaper.pdf.

45 Office of Management and Budget, 2024 Report on the *Cybersecurity Posture of the United States*, May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

46 U.S. Government Accountability Office, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," *GAO WatchBlog*, April 22, 2021, accessed September 22, 2024, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

(Terrorism Risk Insurance Act),[47] could provide a crucial backstop for the cyber insurance market while incentivizing organizations to improve their cybersecurity posture while strengthening economic and societal resilience.

To address these multifaceted challenges and enhance our national cybersecurity resilience, we propose the following recommendations:

Recommendation 4.1: Develop a comprehensive system for critical asset identification and prioritization

This recommendation calls for the establishment of a robust system to identify and prioritize critical entities, with a particular focus on Systemically Important Entities. This system, to be developed and maintained by CISA, should define clear rules, benefits, and burdens for designated entities. The system should define clear rules, benefits, and burdens for designated entities. Benefits might include enhanced government support, access to threat intelligence, and participation in specialized cybersecurity programs. Conversely, SIEs may be required to meet more stringent security standards and reporting requirements.

Implementing this system will provide a clear framework for allocating resources and prioritizing cybersecurity efforts across various sectors. It will also facilitate more targeted and effective collaboration between the public and private sectors in protecting our most critical infrastructure.

Recommendation 4.2: Develop comprehensive cloud security and resilience standards and certification processes

This recommendation emphasizes the need for rigorous standards and certification processes tailored to the unique challenges of cloud environments, particularly for critical infrastructure and SIEs. These standards should address issues such as multi-tenancy risks and supply chain vulnerabilities.

The certification process should be dynamic, incorporating mechanisms for continuous assessment and improvement. This may include requirements for regular third-party audits, penetration testing, and vulnerability assessments. By raising the bar for cloud security, we can ensure that our most critical assets remain protected even as they leverage the benefits of cloud technologies. This should include reviewing the results of the CSIS Commission on Federal Cloud Policy, which assesses how to accelerate and streamline the use of cloud computing and services by federal agencies.

Recommendation 4.3: Establish sector-specific security standards for IT and OT systems

Recognizing the distinct nature of IT and OT environments, this recommendation calls for the development of sector-specific security standards that address both domains. These standards should take into account the unique operational requirements and constraints of each sector, from energy and healthcare to manufacturing and transportation, and recognize that these sectors typically have a mix of regulatory requirements, guidelines, and standards – and gaps where none of these are present. Many OT sectors are regulated for safety and not explicitly for security and data privacy. To be effective in advancing cybersecurity, a holistic understanding of how these guidelines intersect is needed, as well as a shared view among stakeholders of what the end state goal is for a policy architecture to achieve improved cybersecurity.

To drive adoption, we propose creating incentives for critical infrastructure owners and operators to invest in cybersecurity improvements. These could include tax breaks, preferential contracting for entities meeting enhanced standards, or access to specialized government resources and support. The standards should also address both the growing importance of the Industrial Internet of Things in OT environments and requirements that are distinct from IIoT, ensuring that security measures can scale with technological advancements.

Recommendation 4.4: Strengthen societal resilience against malign cyber influence operations

This recommendation advocates for a comprehensive approach to countering malign cyber-influence operations, with a specific focus on adversary actions in cyberspace that aim to undermine public confidence. It calls for the U.S. government to clearly define malign cyber influence operations, distinguishing them from broader misinformation and disinformation concerns. This definition should emphasize the cyber-enabled nature of these threats and their potential impact on national security and democratic processes.

The approach should combine law enforcement efforts with proactive engagement strategies to counter foreign cyber-enabled propaganda and influence campaigns. It emphasizes preserving and enhancing defensive capabilities, including working with allies and partners to identify and disrupt malign actors while also developing offensive capabilities in the information space when necessary and appropriate.

Additionally, it underscores the importance of public awareness and education initiatives to help citizens identify and resist cyber-enabled influence operations. By fostering a more discerning and resilient populace, specifically against

47 U.S. Department of the Treasury, *Terrorism Risk Insurance Program*, accessed September 22, 2024, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program.

cyber-enabled threats, we can significantly reduce the effectiveness of foreign influence campaigns that leverage digital platforms and technologies.

Recommendation 4.5: Examine models for federal government as "Insurer of Last Resort"

This recommendation proposes examining models that position the federal government as an "insurer of last resort" for catastrophic cyber events.[48] Similar to the TRIA model, this approach could provide a crucial backstop for the cyber insurance market, which is facing significant challenges that may lead to a reduction in available coverage.

Key elements of this model should include clearly defined activation thresholds, requirements for insurers to cover a percentage of losses before government assistance activates, a loss-sharing structure, liability caps on governmental exposure, and mechanisms for the government to recoup payments over time. The model should aim to support and stabilize the existing cyber insurance market, not replace it. It should also incorporate a common framework for assessing cyber risks and standards of care for different operational technology verticals. Importantly, entities seeking to benefit from this backstop must first take substantial risk reduction steps, incentivizing improved cybersecurity practices across the board while mitigating moral hazard concerns.

Implementing these recommendations will significantly enhance our national cybersecurity resilience. By adopting a proactive approach to risk reduction, we can better prepare ourselves for the cyber threats of today and tomorrow. This strategy, combining robust standards, targeted incentives, and innovative insurance models, positions us to not only withstand cyber attacks but to rapidly recover and maintain operational continuity in their aftermath.

As we move forward, it's crucial to recognize that cybersecurity is not a static goal but an ongoing process. Regular assessments, continuous improvement, and adaptability will be key to maintaining our cybersecurity posture in the face of emerging threats.

Moreover, enhancing our national cybersecurity resilience is not solely the responsibility of the government or any single entity. It requires a collaborative effort involving public and private sectors, academia, and individual citizens. By working together, sharing information, and collectively raising our cybersecurity standards, we can create a more resilient digital ecosystem that supports our national security, economic prosperity, and societal well-being.

The recommendations outlined in this section provide a roadmap and priorities for strengthening our cybersecurity resilience. By focusing on critical asset protection, cloud security, sector-specific standards, societal resilience, and innovative insurance models, we can build a comprehensive defense against cyber threats. As we implement these measures, we must remain vigilant, adaptable, and committed to continuous improvement in our cybersecurity practices.

48 Sector Down: Ensuring Critical Infrastructure Resilience: Hearing before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, 118th Cong. (2024) (Testimony of Frank Cilluffo) https://homeland.house.gov/hearing/sector-down-ensuring-critical-infrastructure-resilience/.

05 Cyber Statecraft: Navigating International Cyber Challenges

In an increasingly interconnected digital world, the United States faces both unprecedented opportunities and challenges in shaping the international cyber landscape. As cyber threats evolve and transcend national borders, the importance of robust international partnerships and cooperation in cybersecurity has never been more critical. The 2023 Cyber Strategy of The Department of Defense aptly recognizes allies and partners as America's "foundational advantage in the cyber domain," highlighting the need for a comprehensive and coordinated approach to international cyber engagement.[49]

The global cyber environment is characterized by a complex interplay of state and non-state actors, rapidly advancing technologies, and competing visions for the future of the internet. In this context, the United States must leverage its diplomatic, economic, and technological strengths to promote an open, secure, and interoperable global internet while countering authoritarian models that seek to restrict freedom and stifle innovation. This effort requires a multifaceted strategy that encompasses robust cyber diplomacy, active participation in international standards-setting bodies, and close collaboration with like-minded nations and private sector partners.

Central to this endeavor is the role of the U.S. Department of State in spearheading cyber diplomacy efforts.[50] As the primary agency responsible for conducting U.S. foreign policy, the State Department is uniquely positioned to lead in shaping the international cyber environment. However, to fully realize this potential, there is a pressing need to strengthen and expand the department's cyber diplomacy capabilities, ensuring they are commensurate with the growing importance of cyber issues in international relations.

Simultaneously, the United States must redouble its efforts to promote and protect a free, open, and secure internet globally. This vision stands in stark contrast to authoritarian models, exemplified by China's approach, which seeks to exert strict control over information flows and digital infrastructure. By developing and advocating for an affirmative vision of an open internet, the U.S. can help safeguard fundamental freedoms, foster innovation, and promote economic growth on a global scale.

Enhancing international cooperation on cybersecurity standards represents another critical avenue for shaping the global cyber environment.[51] As digital technologies become increasingly integrated into critical infrastructure and everyday life, the importance of robust, widely adopted cybersecurity standards cannot be overstated. The United States must take a leadership role in international standards-setting bodies, leveraging both government expertise and private sector innovation to ensure that emerging standards align with values of openness, security, and interoperability.

It is crucial to recognize that shaping the international cyber environment is not solely the purview of government agencies. Private sector entities, civil society organizations, and individual experts all play vital roles in this ecosystem. Encouraging and facilitating their participation in international forums and standards development processes can significantly amplify the U.S.'s influence and ensure that diverse perspectives are represented.

The interconnected nature of cybersecurity, digital infrastructure policy, and economic development presents both challenges and opportunities. As nations around the world seek to modernize their digital infrastructure, the United States has a strategic interest in promoting secure and reliable solutions. This not only helps allies and partners avoid potentially compromised equipment but also creates economic opportunities for U.S. companies and strengthens global cyber resilience.

Addressing the challenge of attribution in cyberspace requires enhanced international cooperation. Developing mechanisms for sharing intelligence and technical analysis related to cyber incidents with allies and partners can improve collective defense capabilities and serve as a deterrent to malicious actors. Similarly, expanding bilateral and multilateral research and development initiatives on cybersecurity can foster innovation and strengthen ties with key allies.

As we navigate this complex landscape, it is essential to maintain flexibility and adaptability in our approach. The rapid pace of technological change and the evolving nature of cyber threats demand that international cooperation mechanisms be agile and responsive. By fostering a culture of continuous learning and adaptation, the United States can stay at the forefront of global cybersecurity efforts.

49 U.S. Department of Defense, *2023 DoD Cyber Strategy Fact Sheet*, May 26, 2023, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF.

50 U.S. Government Accountability Office, Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities, GAO-24-105563, January 2024, https://www.gao.gov/products/GAO-24-105563. For more information on State Department cyber diplomacy efforts.

51 Natalie Thompson and Mark Montgomery, *Strengthening U.S. Engagement in International Standards Bodies*, Day One Project, June 2021, https://fas.org/wp-content/uploads/2021/06/Strengthening-U.S.-Engagement-in-International-Standards-Bodies.pdf.

In light of these considerations, we propose the following recommendations to enhance the United States' ability to shape the international cyber environment:

Recommendation 5.1: Strengthen the State Department's cyber diplomacy efforts

The Department of State should significantly enhance its cyber diplomacy capabilities to effectively lead U.S. efforts in shaping the international cyber environment. This comprehensive strengthening should begin with the development of a robust international cybersecurity engagement strategy that aligns diplomatic efforts with national security and economic objectives. Such a strategy would provide a cohesive framework for the United States' global cyber engagements, ensuring that diplomatic initiatives are coordinated and mutually reinforcing across different regions and issue areas.

Central to this effort should be an expansion of the role and resources of the Bureau of Cyberspace and Digital Policy.[52] This bureau should be empowered to serve as the focal point for coordinating cyber diplomacy efforts across the U.S. government, as well as engaging with international partners. To support this expanded role, the State Department should increase the number and capacity of cyber attachés at key U.S. embassies. These attachés would play a crucial role in enhancing international cooperation and information sharing on cyber threats and best practices, serving as on-the-ground experts who can build relationships with host country counterparts and facilitate rapid response to emerging cyber issues.

While strengthening the State Department's capabilities, it's essential to foster closer coordination with other agencies that have international cyber programs. For instance, the FBI's cyber attaché program provides valuable law enforcement expertise and connections, while the Department of Defense's cyber capacity-building initiatives offer important military and strategic perspectives. By coordinating these efforts under a unified diplomatic strategy, the United States can leverage the unique capabilities of each agency while presenting a coherent and comprehensive approach to international partners. This coordinated approach would enhance the U.S.'s ability to shape global cyber norms, respond to threats, and build the capacity of allies and partners to secure themselves against cyber threats.

Recommendation 5.2: Promote an open, interoperable internet globally

The United States should lead global efforts to promote and protect a free, open, and secure internet. This initiative should begin with the development and advocacy of an affirmative vision for an open, interoperable, and secure internet in international forums and bilateral engagements. This vision should serve as a counterpoint to authoritarian models of Internet governance, emphasizing the benefits of free information flow, innovation, and respect for individual privacy and human rights.

To support this vision, the U.S. should create programs that actively support internet freedom and combat digital authoritarianism. These programs should be developed and implemented in partnership with like-minded nations and civil society organizations, leveraging a broad coalition to amplify their impact. Such efforts could include providing technical assistance to countries seeking to resist digital authoritarianism, supporting the development of circumvention tools for internet users in repressive environments, and conducting public diplomacy campaigns to highlight the benefits of an open internet.

A key component of this recommendation is the establishment of an international fund to support the development of secure, open-source technologies that promote Internet freedom and interoperability. This fund could provide grants to developers and organizations working on technologies that enhance online privacy, security, and access to information. By promoting open-source solutions, the U.S. can foster a more diverse and resilient global internet ecosystem that is less vulnerable to control by any single entity.

Furthermore, the U.S. should expand cooperation on secure and reliable digital infrastructure to help allies and partners avoid insecure telecommunications equipment. This could involve providing technical assistance, sharing best practices for vendor selection and risk assessment, and potentially offering financing alternatives to help countries resist the allure of cheap but potentially compromised infrastructure options. By helping allies and partners build secure digital foundations, the U.S. can strengthen the global internet's overall resilience and security while promoting its vision of an open and interoperable network.[53]

Recommendation 5.3: Enhance international cooperation on cybersecurity standards

The United States should increase its leadership, participation, consistency, and quality in international standards-setting bodies related to cybersecurity and emerging technologies. To effectively coordinate these efforts across the approximately 19 different agencies involved in international cyber initiatives, a clear "quarterback" role should be established within the U.S. government. This quarterback, potentially positioned within the Office of the National Cyber Director or the National Security Council, would be responsible for aligning and directing U.S. efforts in international cybersecurity

52 U.S. Government Accountability Office, Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities, GAO-24-105563, January 2024, https://www.gao.gov/products/GAO-24-105563. For more information on State Department cyber diplomacy efforts.

53 While securing digital infrastructure is crucial, it's important to balance these efforts with maintaining open data flows. Overly strict data localization policies can sometimes hinder innovation and international collaboration without necessarily improving security.

cooperation and standards development.

This effort should start with a concerted push to increase both U.S. government and private sector participation in international standards development processes, particularly in areas related to critical and emerging technologies. By having a strong presence in these forums, the U.S. can ensure that developing standards align with its values of openness, security, and interoperability. This increased participation is crucial, as other nations have been aggressively promoting their technical standards in these bodies, often outnumbering U.S. representatives by significant margins.

To facilitate this increased participation, the U.S. should create incentives for private sector experts to engage in international standards development processes. These incentives could include grants, tax benefits, or recognition programs that highlight the importance of this work to national security and economic competitiveness. The government should also work to streamline the process for private sector experts to participate in these forums, reducing bureaucratic barriers that might otherwise discourage involvement.

A national program office should be established to identify incentives and remove barriers to participation. This office should develop approaches to incentivize consistent, long-term participation by technical experts from National Labs, universities, and other research institutions, focusing particularly on emerging technologies prior to commercialization.

The CHIPS Act provides a valuable opportunity to support U.S. leadership in international standards and cybersecurity cooperation.[54] Funds and programs established under this act should be leveraged to bolster U.S. expertise in key technology areas and support participation in international standards forums. This approach can help ensure that U.S. technological leadership translates into influence over the global standards that will shape the future of cybersecurity and emerging technologies.

In line with the National Standards Strategy for Critical and Emerging Technology,[55] efforts should be made to enhance U.S. and like-minded nations' representation and influence in international standards governance and leadership. This could involve coordinated campaigns to secure key positions in standards organizations, as well as efforts to build coalitions around shared interests and values in the standards-setting process.

Finally, the U.S. should expand bilateral and multilateral research and development initiatives on cybersecurity with key allies. Programs like the Israel-U.S. Binational Industrial Research and Development Cyber program provide a model for collaborative innovation in cybersecurity.[56] By replicating and expanding such programs with other allies, the U.S. can accelerate the development of cutting-edge cybersecurity technologies while strengthening diplomatic ties and promoting a shared vision of cybersecurity.

The designated quarterback would be responsible for overseeing these various initiatives, ensuring coherent strategy implementation, and serving as the primary point of contact for both interagency coordination and private-sector engagement on international cybersecurity matters. This coordinated approach will help eliminate redundancies, ensure consistent messaging across agencies, and maximize the impact of U.S. efforts in shaping the international cybersecurity landscape.

By implementing these recommendations, the United States can strengthen its position as a global leader in cybersecurity, promote its values and interests in the digital realm, and foster a more secure and prosperous international cyber environment. This approach recognizes the interconnected nature of global cybersecurity challenges and leverages the full spectrum of U.S. capabilities – diplomatic, economic, and technological – to shape a positive future for the global internet.

54 The White House, FACT SHEET: CHIPS and Science *Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China*, August 9, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

55 U.S. Government, *National Standards Strategy for Critical and Emerging Technology*, May 2023, https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf.

56 U.S. Department of Homeland Security, *BIRD Homeland Security Program*, updated July 3, 2024, accessed September 22, 2024, https://www.dhs.gov/science-and-technology/bird-hls.

06 Building Cyber Capacity: Strategies for a Robust Cybersecurity Workforce

Developing, expanding, and maintaining a skilled cybersecurity workforce is a critical national security imperative. The United States faces a severe shortage of cybersecurity professionals, with hundreds of thousands of positions unfilled across both the public and private sectors.[57] This shortage poses significant risks to our national security, economic prosperity, and ability to innovate in an increasingly digital world. Addressing this challenge requires a comprehensive and multi-faceted approach that focuses on removing barriers to workforce mobility, improving education and training programs, enhancing scholarship initiatives, and promoting diversity in the field. This approach aligns with and builds upon the Office of the National Cyber Director's National Cyber Workforce and Education Strategy,[58] which emphasizes the importance of developing a skilled and diverse cybersecurity workforce.

The cybersecurity workforce shortage is not merely a matter of numbers; it's also about having the right mix of skills and expertise to address the complex and evolving nature of cyber threats. From defending critical infrastructure to protecting sensitive data and responding to sophisticated cyber attacks, the demands on cybersecurity professionals are constantly adapting. Additionally, all professions, from engineering to accounting to nursing, need professionals who understand how cybersecurity applies to the digital systems that are now an inherent part of their professions. Programs like the implementation of the National Cyber-Informed Engineering Strategy[59] and its focus on inculcating cybersecurity principles in engineering design represent an exemplar of best practices for driving cyber into the practices and requirements of disciplines. This reality necessitates a workforce that is not only larger but also more flexible, diverse, and continuously learning.

The severe shortage of qualified professionals disproportionately affects smaller and rural organizations. This shortage is twofold: these entities often lack the financial resources to compete for scarce cybersecurity talent, and the limited pool of available professionals tends to gravitate toward larger, more urban organizations offering competitive salaries and career advancement opportunities. As a result, smaller and more rural organizations frequently find themselves without adequate cybersecurity expertise, leaving them arguably more vulnerable to attacks. This vulnerability extends beyond the individual organizations by creating potential weak links in larger supply chain networks. The ripple effects of these vulnerabilities can cascade through sectors and the economy.

Another obstacle is the lack of mobility between public and private sector roles. Currently, there are substantial barriers that prevent cybersecurity professionals from easily transitioning between government and industry positions. This lack of mobility limits the cross-pollination of ideas and experiences that could greatly benefit both sectors. It also restricts the ability of the government to tap into the expertise of private sector professionals during times of crisis or for specific high-priority projects.

The education and training pipeline for cybersecurity professionals also needs attention. Currently, a lack of standardized cybersecurity education at the K-12 level limits the pipeline of future cyber professionals. At the higher-education level, programs like the CyberCorps, the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program.[60] Scholarships for Service have been effective and are continuing to evolve, they are also limited in scale and scope and are challenged to keep pace with the emerging range of cybersecurity specialties needed in today's workforce.

Furthermore, rapidly evolving cyber threats mean that cybersecurity education cannot stop at formal schooling. There's a critical need for continuous learning and upskilling throughout a cybersecurity professional's career. This need for lifelong learning poses challenges for both individuals and organizations in terms of time, resources, and access to cutting-edge training.

Diversity in the cybersecurity workforce is another crucial area that requires attention. The field currently suffers from a lack of diversity in terms of gender, race, and background. This lack of diversity not only limits the pool of available talent but also narrows the range of perspectives and ideas brought to bear on cybersecurity challenges. A more diverse workforce can lead to more innovative solutions and a better understanding of the wide range of users and systems that need protection.

57 CyberSeek, *Cybersecurity Supply/Demand Heat Map*, accessed September 22, 2024, https://www.cyberseek.org/heatmap.html.

58 Office of the National Cyber Director, Initial Stages of Implementation of the National Cyber Workforce and Education Strategy, June 25, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf.

59 U.S. Department of Energy, *National Cyber-Informed Engineering Strategy*, June 2022, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

60 National Security Agency, "Centers of Academic Excellence," accessed September 22, 2024, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

To address these challenges, we propose a series of recommendations aimed at strengthening and expanding the cybersecurity workforce:

Recommendation 6.1: Develop support mechanisms for smaller and rural organizations to access cybersecurity expertise, such as creating virtual CISO organizations

Virtual CISO organizations can provide on-demand cybersecurity leadership and guidance to organizations that cannot afford full-time security executives. This model allows for the sharing of expertise across multiple entities, ensuring that even smaller organizations can benefit from high-level cybersecurity guidance and strategy. Through a mix of public-private collaboration involving NGOs, private sector organizations, and government entities where appropriate, these virtual CISO organizations can be established to meet the varied needs of different sectors. Pooling resources and expertise can help level the playing field for smaller entities while also enhancing the nation's overall cybersecurity posture.

Recommendation 6.2: Create a flexible volunteer system that allows cybersecurity professionals to contribute their skills during crises or for specific projects

This system, which could be termed the Cyber Civilian Response Corps, would allow for the rapid mobilization of private-sector talent to address public-sector cybersecurity needs without the formal structure of a military reserve. Such a program would provide crucial support during crises, similar to how FEMA musters outside help during natural disasters, while also fostering greater collaboration and understanding between the public and private sectors. It could also serve as a bridge between sectors, allowing for knowledge transfer and the continued development of shared best practices. Recent efforts, such as the Franklin Project[61] and Craig Newmark's Volunteer Network for Civil Cyber Defense initiative,[62] demonstrate the growing recognition of the need for and potential impact of coordinated volunteer cybersecurity efforts.

Recommendation 6.3: Implement policies that allow for more flexible employment arrangements, such as part-time government service or short-term assignments for private sector experts

These flexible arrangements would enable cybersecurity professionals to contribute their skills and knowledge to government projects without requiring a full-time commitment, thereby increasing the pool of available talent for critical public sector initiatives. This could include policies for sabbaticals, job rotations, or project-based assignments that allow professionals to move between sectors more easily. Such flexibility could also help in retaining talent by offering diverse career experiences and opportunities for growth.

Recommendation 6.4: Develop a national K-12 cybersecurity curriculum to build a pipeline of future cyber professionals and cyber literate citizens

A comprehensive K-12 cybersecurity curriculum would introduce students to key concepts and skills early on, fostering interest in the field and preparing them for future careers in cybersecurity. This aligns with the Office of the National Cyber Director's vision for comprehensive K-12 cybersecurity education as outlined in the National Cyber Workforce and Education Strategy.[63] This early exposure is crucial for building a diverse and robust talent pipeline, not to mention a better cyber-literate citizenry. The curriculum should be designed to be engaging and relevant, incorporating hands-on activities and real-world examples to spark interest in cybersecurity from an early age. It should also aim to develop not just technical skills but also critical thinking, problem-solving, and ethical decision-making abilities that are crucial in cybersecurity roles. Importantly, this curriculum should be inclusive and engaging for neurodiverse individuals, recognizing the unique strengths and perspectives they can bring to the cybersecurity field. There are a number of existing programs that could be leveraged to take advantage of current work in this area, including the educational programs of the National Cryptologic Foundation[64] and the Alabama School of Cyber Technology and Engineering.[65]

61 Christian Vasquez, "How Benjamin Franklin Is Inspiring Defenders to Protect Critical Infrastructure," CyberScoop, August 30, 2024, accessed September 22, 2024, https://cyberscoop.com/franklin-project-cybersecurity-volunteers-jeff-moss-def-con/.

62 Tonya Riley, "Newmark Initiative Will Bring Online a Network of Civil Defense Hackers," CyberScoop, September 20, 2023, accessed September 22, 2024, https://cyberscoop.com/berkeley-volunteer-network-civil-cyber/.

63 Office of the National Cyber Director, Initial Stages of Implementation of the National Cyber Workforce and Education Strategy, June 25, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf.

64 National Cryptologic Foundation, "Educators & Students," accessed September 22, 2024, https://cryptologicfoundation.org/educators/.

65 Alabama School of Cyber Technology and Engineering, "Home," accessed September 22, 2024, https://www.ascte.org/.

Recommendation 6.5: Expand existing programs like CyberCorps, Scholarship for Service, and the National Centers of Academic Excellence in Cybersecurity program to cover a wider range of cybersecurity specialties and educational levels

By broadening the scope of these scholarship and academic excellence programs, we can attract a more diverse pool of candidates and address the need for specialized skills in emerging areas of cybersecurity. This expansion should include support for associate's degrees, certifications, and other non-traditional educational paths, recognizing that valuable cybersecurity skills can be developed through various routes. The expanded programs should also focus on areas of critical need, such as industrial control systems security, engineering, artificial intelligence in cybersecurity, and secure software development.

Recommendation 6.6: Evolve and expand post-service placement programs to help scholarship recipients transition into key cybersecurity roles in government and critical infrastructure sectors

This onboarding effort can help bridge the gap between education and employment, ensuring that newly trained cybersecurity professionals are effectively integrated into the workforce where their skills are most needed. This effort could also include a focus on retaining talent in critical roles through continued professional development opportunities or incentives for long-term commitment to public sector positions. A veterans assistance program could ensure that the nearly 200,000 transitioning military service members have an opportunity to use their skills as cyber-enabled warriors to gain entry into the federal, or state and local cyber civilian workforce. A more holistic and strategic focus will improve the return on investment for these programs.

Addressing the cybersecurity workforce shortage is a complex challenge that requires a comprehensive, collaborative, and forward-looking approach. By implementing the above recommendations, we can build a more robust, diverse, and flexible cybersecurity workforce capable of meeting the evolving challenges of the digital age. This approach will not only enhance our national security posture but also drive innovation and economic growth in the cybersecurity sector.

The development of a strong cybersecurity workforce is not just about filling current job openings; it's about creating a sustainable pipeline of talent that can adapt to future challenges. It also requires a cultural shift that places cybersecurity at the forefront of our educational and professional development priorities. By investing in our cybersecurity workforce, we are investing in the resilience and security of our country now and in the future.

This is a critical undertaking that will require sustained commitment and collaboration across government, industry, and academia. The benefits in terms of enhanced security, economic competitiveness, and technological leadership make it an essential priority for the incoming administration. As we move forward, it will be crucial to regularly assess and adapt these initiatives to ensure they continue to meet the evolving needs of the cybersecurity field and the nation as a whole.

07 Securing the Future: Safeguarding Critical and Emerging Technologies

The United States faces both great opportunities and significant challenges in maintaining its global leadership in critical and emerging technologies. These technologies, including artificial intelligence, quantum computing, and advanced semiconductors, have profound implications for national security. As such, it is imperative that the United States adopt a comprehensive, strategic, and proactive approach to identifying, protecting, and promoting its leadership in these key areas while simultaneously addressing the associated cybersecurity risks.

The U.S. government has already taken important steps in this direction, such as the issuance of National Security Memorandum 10, which mandates the implementation of quantum-resistant cryptography across government systems.[66] Additionally, National Security Memorandum 33 has addressed the critical issue of research security, aiming to protect America's research enterprise from foreign interference and exploitation while maintaining an open and collaborative scientific environment.[67]

The landscape of critical and emerging technologies is constantly evolving, necessitating a dynamic and adaptable strategy.[68] Currently, the U.S. government's approach to managing these technologies is fragmented, with multiple agencies maintaining separate lists and oversight mechanisms. Also, government budget cycles also slow down agility in meeting emerging challenges. This disjointed approach hinders effective coordination and can lead to gaps in protection or, conversely, unnecessary duplication of efforts. To address this, a unified and comprehensive approach is essential.

One of the primary challenges in this domain is the identification and protection of critical technologies. The current system, where multiple agencies such as the Departments of Commerce and State, as well as the Intelligence Community, maintain separate lists, is inefficient and potentially leaves vulnerabilities. A consolidated, authoritative list managed by a single entity would significantly enhance the government's ability to protect these crucial technologies and ensure a coordinated response across all relevant agencies.

An emerging concern in this landscape is the potential exploitation of early-stage investment processes in critical technology startups. While mechanisms like the Committee on Foreign Investment in the United States provide oversight for many foreign investments, there may be loopholes in early-stage funding that could allow adversarial nations to gain access to critical technologies. This issue is particularly pertinent for cybersecurity and other advanced technology startups, where even minority investments in venture capital funds could have significant national security implications. Addressing these vulnerabilities requires a delicate balance between maintaining an open investment environment that fosters innovation and ensuring that critical technologies are adequately protected from potential exploitation by foreign adversaries.

Moreover, the rapid pace of technological innovation requires a continuous assessment of emerging technologies and their potential national security implications. This ongoing evaluation is crucial not only for updating protection lists but also for informing policy decisions and research priorities. It's also equally important to establish clear criteria for removing technologies from protection lists when appropriate to avoid stifling innovation and economic growth.

The security of technology supply chains is another critical aspect that demands immediate attention. Recent global events, including the COVID-19 pandemic and geopolitical tensions, have highlighted the vulnerabilities in our current supply chain systems, particularly for critical components and technologies. Supply chain security is not a future problem; we are operating in a compromised environment today. Consequently, a national strategy for securing technology supply chains and making sure critical elements are available is essential, focusing not only on critical components but also on reducing dependence on potentially adversarial nations through reshoring or friend-shoring initiatives.

Emerging technologies, particularly in the realm of quantum computing, pose unique challenges to our current cybersecurity paradigms. The potential of quantum computers to break many of our current encryption methods necessitates a proactive approach to developing and implementing quantum-safe cryptography. This transition is not a simple task and requires a comprehensive evaluation at the programmatic level across government systems and critical infrastructure.

To maintain its technological edge, the United States must also focus on promoting leadership in key technology areas.

66 The White House, *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

67 The White House, *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

68 Frank Cilluffo, "Unpacking the National Cyber Director's Posture Report," *The Cipher Brief*, May 7, 2024, accessed September 22, 2024, https://www.thecipherbrief.com/column_article/unpacking-the-national-cyber-directors-posture-report.

The CHIPS and Science Act[69] and other recent legislation represent a crucial, strategic reversal in the decades-long erosion of U.S. national research and development spending. We need to not only continue rebuilding our national investment in R&D and developing our nation's R&D infrastructure but also ensure that technology investments include requirements for security and resilience. This involves not just increased funding for research and development but strategic investment in areas that will secure America's competitive advantage. However, this investment must be balanced and coordinated to avoid duplication of efforts and ensure maximum impact.

In light of these challenges and opportunities, we propose the following recommendations:

Recommendation 7.1: Evolve and unify national lists for critical and emerging technologies list and prohibited entities

Critical and Emerging Technologies List

The Office of Science and Technology Policy, in collaboration with the Department of Commerce and other relevant agencies, should evolve and maintain a unified list of critical and emerging technologies.[70] This effort should incorporate insights from existing initiatives, such as the National Academies of Sciences, Engineering, and Medicine's study to refresh the "Cyber Hard Problem List."[71] This consolidated list will serve as a crucial tool for identifying and prioritizing technologies that are vital to U.S. national security, economic resilience, and economic competitiveness. A cross-agency task force should be created to continuously assess and update this list, evaluating new technologies and their potential implications. Clear criteria and processes for adding to and removing technologies from the list must be established, striking a balance between protection needs and innovation concerns.

Prohibited Entities List

Separately, the Department of Commerce should consolidate existing lists of prohibited entities into a single, authoritative list. This list will identify companies, organizations, and individuals that pose security risks or are subject to restrictions due to national security concerns. The consolidation will enhance coordination across government agencies and simplify industry compliance.

To ensure the ongoing relevance and effectiveness of both lists, regular updates will be essential to reflect the rapidly evolving technological and geopolitical landscape. These lists should be considered holistically in developing national priorities and enhancing supply chain security efforts. This approach will ensure that the United States remains proactive in identifying and protecting critical technologies while also maintaining clear guidelines on restricted entities.

Recommendation 7.2: Enhance supply chain security for critical technologies

A comprehensive national strategy for securing technology supply chains should be implemented, with a particular focus on critical components and technologies, including software. This strategy should include the development of incentives for reshoring or friend-shoring production of critical technology components, reducing dependence on potentially adversarial nations.[72] Additionally, standards and certification processes for supply chain and software security should be created, which can be used in federal procurement and recommended for private sector adoption. These standards would provide a benchmark for security practices across the supply chain, enhancing overall resilience. The strategy should also establish a framework for illumination, continuous monitoring, and assessment of supply chain risks in critical technology areas across a range of risk factors, allowing for rapid identification and mitigation of vulnerabilities as they emerge and an implied requirement to address them. As part of this effort, priority should be given to the effective implementation of the Federal Acquisition Security Council's responsibilities for critical and emerging technologies, leveraging its statutory mandate to achieve effective supply chain threat information sharing and procurement security.[73]

Recommendation 7.3: Develop a quantum-safe cryptography transition plan

A comprehensive plan for transitioning government systems and critical infrastructure to quantum-safe cryptography is essential. This plan should begin with a thorough assessment of current systems and infrastructure to identify vulnerabilities to quantum computing attacks. Based on this assessment, agency-specific plans for transitioning to post-quantum encryption should be developed, addressing unique challenges and timelines for each agency. The plan should establish clear milestones and deadlines for the implementation of quantum-safe cryptography across

69 *CHIPS and Science Act of 2022*, Public Law No. 117-167, 136 Stat. 1366 (2022), https://www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf.

70 National Science and Technology Council, *Critical and Emerging Technologies List Update*, February 2024, https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf.

71 National Academies of Sciences, Engineering, and Medicine, *Cyber Hard Problems*, accessed September 22, 2024, https://www.nationalacademies.org/our-work/cyber-hard-problems.

72 In implementing supply chain security measures, care should be taken to avoid unnecessary restrictions on data flows, especially among trusted allies. The goal is to enhance security without compromising the benefits of global digital collaboration.

73 FASC was created in statute but has not yet fulfilled its intent and potential to achieve effective supply chain threat information sharing and procurement security.

different sectors and systems, ensuring a coordinated and timely transition. Adequate resources must be allocated for research, development, and implementation of quantum-safe cryptographic solutions, recognizing that this transition is a significant undertaking that requires substantial investment in both technology and expertise.

Recommendation 7.4: Promote U.S. leadership in key technology areas

To maintain and enhance U.S. leadership in critical technologies such as AI, 5G, 6G, quantum computing, and advanced semiconductors, a national strategic investment plan should be developed and implemented. This plan should build on existing federal government R&D coordination by the National Science and Technology Council and OSTP and evolve to engage the national R&D enterprise more effectively. Accordingly, this plan should increase federal funding for research and development in these key areas, ensuring judicious allocation of funds to maintain U.S. leadership. A national-level coordination body for R&D efforts in critical and emerging technologies across government agencies, industry, and academia should be established to minimize duplication and maximize impact. This body would help align research priorities, facilitate development and access to national testing and evaluation infrastructure, facilitate information sharing, and ensure that resources are used efficiently across a range of key technology areas, including but not limited to cybersecurity. The plan should also focus on developing partnerships with allies and like-minded nations to pool resources and expertise in critical technology development, recognizing that international collaboration can accelerate progress and strengthen our collective technological capabilities. Finally, the plan should create incentives for private sector investment and innovation in key technology areas, fostering a robust ecosystem of research, development, and commercialization that keeps the United States at the forefront of technological advancement.

By implementing these recommendations, the United States can strengthen its position as a global leader in critical and emerging technologies while simultaneously enhancing its cybersecurity and supply chain security posture. This approach will not only protect our national interests but also drive economic growth and innovation in the coming decades.

The challenges we face in the realm of critical and emerging technologies are complex and multifaceted. They require a coordinated, strategic approach that balances the need for protection with the imperative of innovation. By consolidating our efforts, securing our supply chains, preparing for the quantum future, and strategically investing in key areas, we can ensure that the United States remains at the forefront of technological advancement while safeguarding our national security interests.

As we move forward, it is crucial that we remain adaptable and responsive to the ever-changing technological landscape. The recommendations outlined here provide a framework for action, but their successful implementation will require ongoing commitment, collaboration across sectors, and a willingness to evolve our strategies as new challenges and opportunities emerge.

08 Foundations of Cyber Resilience: Resources, Economy, and Continuity

The rapidly evolving cyber threat landscape has underscored the need for the U.S. government to be properly organized and adequately resourced to safeguard America's national security and economic stability. Cybersecurity policies are of strategic importance and are foundational to the safe functioning of government, critical infrastructure, and the private sector; they should also ensure the continuity of the economy during significant cyber disruptions. Sector Risk Management Agencies responsible for coordinating critical infrastructure cybersecurity often struggle to provide necessary guidance and support to critical infrastructure owners and operators due to insufficient funding. Without proper resourcing and defined baseline capabilities, SRMAs are unable to fulfill their duties effectively, undermining the nation's overall cybersecurity posture.

There is a need to review and potentially rationalize the number of sectors where CISA serves as SRMA. Currently, CISA is responsible for multiple critical infrastructure sectors, which may strain its resources and dilute its effectiveness. A comprehensive review of critical infrastructure designations and SRMA assignments should be conducted to ensure that each sector receives adequate attention and that CISA's roles as National Coordinator and SRMA are clearly delineated and properly resourced.

Effective cybersecurity management hinges on a critical triad: authority, accountability, and resources. Agencies and agency leaders must have the authority to implement necessary measures, be held accountable for outcomes, and be provided with sufficient resources to execute their responsibilities.

The misalignment between policy objectives and funding is a recurring issue that compromises the effectiveness of national cybersecurity efforts. While the Biden administration has announced a $13 billion investment in cybersecurity for federal civilian agencies in Fiscal Year (FY) 2025, this funding is undermined by critical gaps in allocation.[74] Recent appropriations have included notable investments like $2.8 billion for the Cybersecurity and Infrastructure Security Agency,[75] but funding for SRMAs remains uneven, often failing to support interagency efforts and collaboration with critical infrastructure owners and operators. These budgetary shortfalls reflect a broader failure among federal agencies to fully recognize their responsibilities.

Several agencies face significant budgetary shortfalls. In 2023, the Administration for Strategic Preparedness and Response (ASPR), housed within the U.S. Department for Health and Human Services, received $708,000 for SRMA responsibilities. In the FY2024 budget request, ASPR requested a $7 million increase. While, the agency did ultimately get that increase, it was already the spring of 2024 when Congress passed full-year appropriations, meaning the FY2025 request used the FY2023 enacted numbers and the Continuing Resolution as the baseline. Therefore, the FY2025 request for a $12 million increase, is a $5 million increase over the FY2024 enacted numbers. The U.S. Department of Agriculture has requested only an additional $500,000 in FY2025 and one full-time employee to support its sector risk management responsibilities.

The Environmental Protection Agency also faces a similar fate. Four years ago, the Cyberspace Solarium Commission recommended $45 million budget as the SRMA for water and wastewater sector cybersecurity support,[76] but EPA only provided $11.8 million in funding for FY23, and this is to support 52,000 drinking water and 16,000 wastewater systems, most of which service small- to medium-sized communities of less than 50,000 residents.

Most concerning of all is that the current budget proposal contains no dedicated funding for the U.S. Coast Guard to safeguard the maritime transportation systems subsector despite the fact that the recent Executive Order 10173[77] expanded and clarified the Coast Guard's roles and responsibilities in protecting vessels, harbors, ports, and waterfront facilities from cyber threats. The Coast Guard needs proper resources and personnel to implement the increased requirements.

Despite these problems, there is some good news for critical infrastructure resourcing. The SRMA for the energy sector, the Office of Cybersecurity, Energy Security, and Emergency Response at the Department of Energy, saw a steady funding of $200 million in FY25. With these funds, they are able to offer grant programs, provide training, and conduct exercises and research that support the sector's cybersecurity.

These funding inconsistencies overlook essential programs that aim to strengthen the cyber resilience of U.S. critical infrastructure, which remains vulnerable to cyber threats by adversaries. The failure to define baseline capabilities and adequately resource SRMAs and other key cybersecurity

74 Office of Management and Budget, *Analytical Perspectives: Budget of the U.S. Government, Fiscal Year 2025*, March 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/ap_15_it_fy2025.pdf.

75 U.S. Department of the Interior, *President Biden's Budget Invests $2.8 Billion to Support Economies, Outdoor Recreation and Access to Public Lands*, June 3, 2021, https://www.doi.gov/pressreleases/president-bidens-budget-invests-28-billion-support-economies-outdoor-recreation-and.

76 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, March 2020, http://cybersolarium.org/.

77 The White House, *Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States*, February 21, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/21/executive-order-on-amending-regulations-relating-to-the-safeguarding-of-vessels-harbors-ports-and-waterfront-facilities-of-the-united-states/.

programs not only affects their immediate operational capabilities but also has long-term implications for national security. Without robust funding, these agencies cannot provide the proactive guidance, threat intelligence, exercises, and support necessary to protect critical infrastructure sectors from increasingly sophisticated cyber threats.

CISA has been designated as the national coordinator for critical infrastructure security and resilience under the National Security Memorandum-22. In this role, CISA will ensure SRMAs are fulfilling their responsibilities and identify cross-sector risks. In addition, CISA provides federal civilian government agencies with cybersecurity guidance, technical support, and coordination in working with the private sector. However, for CISA to expand its services effectively and improve its operational capabilities to respond swiftly to emerging threats, enhanced and sustained investment is required.

Furthermore, underfunding of essential programs, such as those supporting foundational research and standards setting, threatens the success of broader cybersecurity efforts. For example, the National Institute of Standards and Technology, tasked with critical roles in developing cybersecurity guidelines and standards, has seen its budget requests consistently fall short. NIST's FY25 budget request proposes only $96.8 million for its cybersecurity and privacy program, below funding levels the Cyberspace Solarium Commission recommended four years ago.[78] This chronic underfunding forces NIST to make difficult choices between maintaining its core responsibilities and addressing new high-priority tasks, ultimately jeopardizing its ability to provide the necessary support to both the public and private sectors.[79] Additionally, efforts to modernize federal IT infrastructure should consider findings from the CSIS Commission on Federal Cloud Policy[80] to optimize resource allocation and improve efficiency in cloud adoption across agencies.

As cyber threats continue to evolve, so too must the strategies that defend against them. There must be a parallel commitment to addressing funding and capability disparities across SRMAs and a renewed focus on strategic planning to enhance coordination among agencies as a core component of national resilience.

One such area for government-led planning is a national Continuity of the Economy plan, which is essential for restoring critical economic functions in the event of a significant cyber disruption or other natural or manmade disaster. Developing a COTE plan requires gaining comprehensive insights through cyber threat intelligence, national-level tabletop exercises, and stakeholder engagements with the private sector and critical infrastructure owners. Although the FY21 NDAA authorized the development of a COTE plan, the report that the administration belatedly delivered to Congress in August 2023 dismissed the need for additional COTE planning.[81] The report brushed aside gaps in current federal incident response capabilities and failed to grapple with the ways the private sector must participate in the development and implementation of the plan. Fortunately, the next administration will have a chance to reassess the prior report since the legislation mandating the original COTE plan requires updates every three years.

It is crucial to align cybersecurity efforts with the congressional calendar to maximize impact and ensure timely action. Key dates in the 119th Congress that will affect cybersecurity policy and funding include committee assignments in January, posture hearings from February to May, the release of the President's Budget in February or March, NDAA member requests due in April, NDAA markups in May/June, and appropriations markups in June/July. The final passage of the NDAA is likely to occur in December. By proactively planning around these dates, the administration can more effectively advocate for and secure the necessary resources for critical cybersecurity initiatives. This approach will help ensure that cybersecurity priorities are properly addressed in both policy discussions and budget allocations throughout the congressional cycle.

To address these crosscutting resource and policy challenges, we propose a series of recommendations aimed at adequately resourcing federal agencies.

Recommendation 8.1: Significantly increase budget and resources for Sector Risk Management Agencies

SRMAs are crucial in coordinating and managing cybersecurity risks across the U.S. critical infrastructure sectors. However, inadequate funding often limits their ability to provide necessary guidance, share threat intelligence, conduct exercises, and support critical infrastructure owners and operators. To enhance the operational effectiveness of SRMAs, it is essential to substantially increase their budgeting and resourcing across the federal government. This increased funding should be specifically targeted towards enhancing SRMA capabilities in threat analysis, information sharing, exercises, and sector-specific support services. Properly resourcing SRMAs to conduct defined baseline capabilities will empower them to fulfill their expanded duties, implement more robust policies, and bolster national resilience against increasingly sophisticated cyber threats. This financial commitment will ensure SRMAs can lead proactive and coordinated efforts to safeguard critical infrastructure, significantly strengthening the overall cybersecurity posture of the United States.

This increase in funding and resources should explicitly address the unique challenges faced by CISA in its role as SRMA for multiple sectors. The allocation should support a comprehensive review of CISA's SRMA assignments, potentially rationalizing the number of sectors under its

78 Office of Management and Budget, *NIST-NTIS FY2025 Congressional Budget Submission*, March 2024, https://www.commerce.gov/sites/default/files/2024-03/NIST-NTIS-FY2025-Congressional-Budget-Submission.pdf.

79 RADM (Ret.) Mark Montgomery and Michael Sugden, "Biden's Cybersecurity Plan has a Huge Funding Gap," The Hill, May 8, 2024, accessed October 14, 2024, https://thehill.com/opinion/cybersecurity/4651731-bidens-cybersecurity-plan-has-a-huge-funding-gap/.

80 James A. Lewis, *Accelerating Federal Cloud Adoption for Modernization and Security*, Center for Strategic and International Studies, July 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230728_Lewis_Federal_CloudAdoption.pdf.

81 Mark Harvey and RADM (Ret.) Mark Montgomery, "After the Attack: A Playbook for Continuity of the Economy Planning and Implementation," Foundation for the Defense of Democracies, September 13, 2023, accessed October 14, 2024, https://www.fdd.org/analysis/2023/09/13/after-the-attack/.

purview and ensuring that CISA has the specific resources needed to effectively fulfill its SRMA duties across all assigned sectors. This targeted approach will help address the strain on CISA's resources and improve its effectiveness in coordinating cybersecurity efforts across its designated critical infrastructure sectors.

Recommendation 8.2: Enhance National Institute of Standards and Technology funding

NIST plays an essential role in developing standards and guidelines used by both the public and private sectors. NIST standards are referenced by other federal standards in the DoD and the IC, and NIST supports the American National Standards Institute,[82] which administers and coordinates the U.S. voluntary standards and conformity assessment system. Despite these numerous unique and critical strategic roles, repeated funding shortfalls have left the agency unable to meet both its traditional cybersecurity responsibilities and new tasks mandated by various executive orders and legislation. For instance, in 2024, NIST struggled to process new additions to its National Vulnerability Database, which records common vulnerabilities and exposures.[83] To ensure NIST can continue leading cybersecurity research and updating and developing essential frameworks, a substantial increase in funding is necessary.

Recommendation 8.3: Resource Cybersecurity and Infrastructure Security Agency and Fund Technology Modernization Funds to Protect Federal Civilian Networks and Critical Infrastructure

CISA plays a critical role in defending federal civilian networks against increasingly complex cyber threats.[84] To effectively fulfill its mission as the national coordinator and lead civilian cybersecurity agency, CISA must be adequately funded and equipped with the necessary resources. This includes not only direct funding for CISA's operations but also continued investments in technology modernization efforts across the federal government. These investments should address both Information Technology and Operational Technology systems, recognizing the critical importance of OT in many sectors of critical infrastructure. Legacy systems across government agencies pose significant security risks, and without proper funding, efforts to secure these systems will continue to fall short. Consider establishing dedicated funding or specific criteria for OT modernization projects within the Technology Modernization Fund to ensure they receive appropriate attention and resources alongside IT initiatives. Robust resourcing for CISA, combined with targeted investments in both IT and OT modernization, will enhance the agency's capacity to detect, mitigate, and respond to cyber incidents across the full spectrum of federal and critical infrastructure systems

Recommendation 8.4: Conduct a robust Continuity of the Economy Planning

The Department of Homeland Security should lead the development of a national Continuity of the Economy (COTE) plan to restore critical economic functions in the event of a significant disruption, including cyberattacks. Effective COTE plan requires information from robust cyber threat intelligence, national-level tabletop exercises, and engagement with the private sector and critical infrastructure owners and operators. This activity should also account for the fact that technology manufacturers and service providers are global. Although previous legislation authorized the development of a COTE plan with triennial updates, the administration's delayed report to Congress in August 2023 downplayed further planning needs. A renewed effort is required.

Addressing these cross-cutting themes is important for strengthening the nation's cybersecurity posture and ensuring economic resilience in the face of evolving cyber threats. The recommendations outlined in this section - significantly increasing resources for Sector Risk Management Agencies, enhancing NIST funding, bolstering CISA's capabilities, and developing a robust Continuity of the Economy plan - form a cohesive strategy to address critical gaps in our current approach.

While extremely important, these measures are not merely about allocating more resources; they represent a fundamental shift in how we conceptualize and prioritize cybersecurity across all sectors of government and the economy.[85] By aligning budgets with strategic priorities, fostering continuity across administrations, and integrating cyber resilience into the fabric of our economic planning, we can create a more robust and adaptive cybersecurity ecosystem.

As we move forward, it is crucial to recognize that cybersecurity is not a static goal but an ongoing process that requires continuous attention, investment, and adaptation. The implementation of these recommendations will require sustained commitment from policymakers, agency leaders, and private sector partners. By addressing these cross-cutting issues, we can build a stronger, more resilient digital infrastructure that not only protects against current threats but is also prepared to face the challenges of tomorrow. This comprehensive approach will be essential in safeguarding America's national security, economic stability, and technological leadership in the years to come.

82 American National Standards Institute, "Home," accessed September 22, 2024, https://www.ansi.org/.

83 Jonathan Greig, "Vulnerability Database Backlog Due to Increased Volume, Changes in 'Support,' NIST Says," *The Record*, April 1, 2024, accessed September 22, 2024, https://therecord.media/vulnerability-database-backlog-nist-support/.

84 Matt Hayden, "Cyberattacks on the U.S. Water Supply – and How to Fight Back," *The Cipher Brief*, April 30, 2024, accessed September 22, 2024, https://www.thecipherbrief.com/column_article/cyberattacks-on-the-u-s-water-supply-and-how-to-fight-back.

85 Frank Cilluffo and Alison King, "How to Fine-Tune the White House's New Critical Infrastructure Directive," *CyberScoop*, May 1, 2024, accessed September 22, 2024, https://cyberscoop.com/how-to-fine-tune-the-white-houses-new-critical-infrastructure-directive/.

Conclusion

As we stand at the precipice of a new era in cybersecurity, the recommendations outlined in this report represent a comprehensive and forward-looking approach to addressing the complex challenges that lie ahead. The digital landscape continues to evolve at an unprecedented pace, presenting both opportunities and threats that demand our immediate attention and strategic response. This task force report, drawing upon the collective expertise of leaders across government, industry, and academia, provides a roadmap for enhancing our nation's cyber resilience and maintaining our competitive edge in an increasingly interconnected world.

The recommendations span a wide range of critical areas, from regulatory harmonization and strengthening multi-stakeholder collaboration to enhancing our deterrence capabilities and building a robust cybersecurity workforce. Each of these areas is integral to our overall cybersecurity posture, and progress in one domain will inevitably strengthen our position in others. However, it is crucial to recognize that these recommendations are not isolated solutions but interconnected components of a holistic strategy.

One of the key themes that emerges throughout this report is the need for greater coordination and collaboration across all sectors. The challenges we face in cyberspace transcend traditional boundaries between government agencies, private industry, and international partners. Our recommendations for strengthening multi-stakeholder collaboration, particularly in operationalizing public-private partnerships, reflect this reality. By fostering closer ties between government entities like CISA, the FBI, and the NSA with private sector partners, we can create a more robust and responsive cyber ecosystem capable of addressing threats in real time.

Another critical aspect highlighted in this report is the importance of proactive measures in cybersecurity. Our recommendations for enhancing deterrence capabilities and imposing costs on adversaries in cyberspace reflect a shift from a purely defensive posture to a more assertive offensive strategy. This approach, somewhat encapsulated in the "defend forward" strategy, recognizes that in the digital domain, the best defense often requires a strong offense. However, it is crucial that these efforts are carefully calibrated and executed within a clear legal and ethical framework to avoid unintended escalation.

The report also underscores the critical importance of building and maintaining a skilled cybersecurity workforce. The recommendations for expanding educational programs, creating flexible employment arrangements, and developing support mechanisms for smaller organizations address the current shortage of cybersecurity professionals. These initiatives are not just about filling current job openings; they are about creating a sustainable pipeline of talent that can adapt to future challenges and drive innovation in the field.

In addressing emerging technologies, our recommendations highlight the need for a balanced approach that promotes innovation while safeguarding national security interests. The proposals for establishing a unified critical technologies list and enhancing supply chain security reflect an understanding that technological leadership is intrinsically linked to national security in the 21st century. By taking a proactive stance in areas like quantum-safe cryptography, we can ensure that our cybersecurity measures remain effective in the face of rapidly advancing technologies.

The cross-cutting themes of resource allocation, economic resilience, and continuity of effort serve as the foundation upon which our other recommendations are built. The call for increased funding for Sector Risk Management Agencies and key institutions like NIST reflects an understanding that effective cybersecurity requires sustained investment. Similarly, the emphasis on developing a robust Continuity of the Economy plan recognizes that cyber resilience is not just about protecting individual systems but ensuring the stability of our entire economic infrastructure in the face of significant disruptions.

It is crucial to recognize that cybersecurity is not a static goal but an ongoing process that requires continuous adaptation and innovation. The threat landscape is constantly evolving, and our strategies must evolve with it. This will require sustained commitment from policymakers, agency leaders, and private sector partners, as well as a willingness to reassess and adjust our approaches as new challenges emerge.

Moreover, while this report provides a comprehensive set of recommendations, it should be viewed as a starting point rather than an endpoint. The rapidly changing nature of cyber threats means that we must remain vigilant and open to new ideas and approaches. Regular assessments and updates to our strategies will be essential to ensure their continued relevance and effectiveness.

The recommendations put forth in this report reflect a nuanced understanding of the complex challenges we face and provide a roadmap for addressing them. However, the true measure of their success will lie in their implementation. It will require leadership, resources, and a shared commitment across all sectors of society to turn these recommendations into reality.

As we move forward, we must remember that cybersecurity is not just a technical challenge but a strategic imperative that touches every aspect of our national security and

economic prosperity. By adopting a proactive, collaborative, and adaptive approach to cybersecurity, we can build a more resilient digital infrastructure that not only protects against current threats but is also prepared to face the challenges of tomorrow. In doing so, we can ensure that the United States remains at the forefront of the digital revolution, securely harnessing the power of technology to drive innovation, economic growth, and national security in the years to come.

Task Force Members

The task force assembled for this cybersecurity report represents a diverse and highly accomplished group of professionals from across the public and private sectors. Drawing upon decades of collective experience in national security, cybersecurity, technology, and policy, this team brought together a wealth of expertise to address the complex challenges facing the United States in the digital domain.

The collaborative nature of the task force's work is evident in the breadth and depth of the recommendations presented in this report. Through a series of meetings, discussions, and workshops, the task force members engaged in rigorous debate and analysis, drawing upon their varied backgrounds to identify key challenges and develop innovative solutions. The process involved synthesizing complex technical concepts with policy considerations, ensuring that the recommendations are both technically sound and practically implementable. The task force's approach reflects a commitment to addressing cybersecurity challenges holistically, recognizing the interconnected nature of digital threats and the need for coordinated responses across sectors and agencies. Below is a list of the members and links to their respective bios.

Frank Cilluffo
RADM Mark Montgomery (Ret.)
George Barnes
Joshua Whitman, PhD
Ben Bass
Thomas P. Bossert
David Bowdich
Stephen Boyd
Cheri Caddy
Chris Cummiskey
Michael Daniel
Chuck Durant
Michael D'Ambrosio
William Evanina
Ernest Ferraresso
Preston Golson
Katherine Gronberg
Michele Guido
Brian Harrell
Melissa Hathaway
Matt Hayden
Suzanne Wilson Heckenberg
Andrew Howell
Daniel Kaniewski
John Katko
Brian Keeter
Steve Kelly
Alison King
Rob Knake
Bob Kolasky
Kate Ledesma
Brad Medairy
Christopher Porter
Christopher Roberti
Bradon Rogers
Jordana Siegel
Kiran Sridhar
Kiersten Todt
Bryan Ware
Mark Weatherford

Disclaimer - While this report represents the collective effort of the task force, the views and recommendations expressed herein do not necessarily reflect the official positions of the organizations or companies with which individual task force members are affiliated. Task force members participated in their personal capacities, contributing their expertise to this collaborative effort.

