CSC 2.0

September 2024

2024 Annual Report on Implementation

Jiwon Ma
RADM (Ret.) Mark Montgomery

Table of Contents

Executive Summary

The cyber threat to America's national critical infrastructure has expanded since the U.S. Cyberspace Solarium Commission (CSC) issued its original March 2020 report. The threat comes from both nation-state adversaries, such as the Volt Typhoon attacks from China, and from criminals, who are escalating ransomware attacks, with a 74 percent increase in the number of reports in 2023.[1] The vulnerabilities inherent in our highly networked infrastructures amplify the risk posed by such threats.

To date, about 80 percent of the Commission's original 82 recommendations have been fully implemented or are nearing implementation, and an additional 12 percent are on track to be implemented, a testament to the concerted efforts of the executive branch and Congress in the cybersecurity domain. While most of these recommendations were accomplished through legislation or policies similar to those suggested by the Commission, others were addressed, or are being addressed, by the administration or Congress using innovative solutions not initially considered by the Commission. This adaptability and creativity are commendable and further enhance the outcomes.

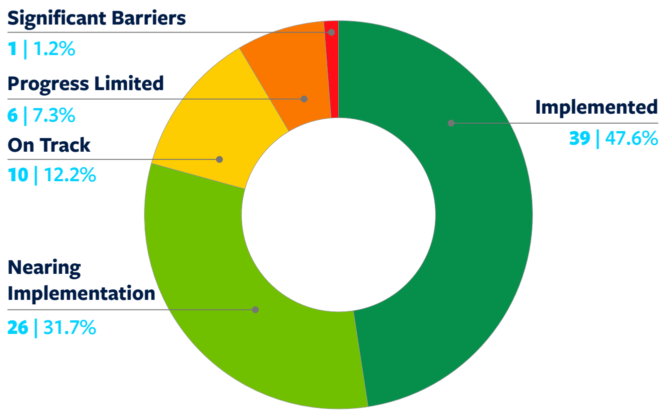
The executive branch leads the effort to achieve a unified cyber defense against malign cyber actors and establish deterrence in cyberspace. The Office of the National Cyber Director (ONCD), now led by the second Senate-confirmed national cyber director, Harry Coker, Jr., has been a key force in leading the development and implementation of a whole-of-government approach to cybersecurity policies. Administration efforts include:

- The ONCD completed 33 of the 36 initial initiatives to implement the National Cybersecurity Strategy published in March 2023.
- The White House issued a new national security memorandum on critical infrastructure security and resilience (NSM-22), creating a national risk management cycle.
- NSM-22 appointed the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for the security and resilience of critical infrastructure and mobilized sector risk management agencies to better support private sector partners.
- Under Director Jen Easterly, CISA's capacity continues to increase, with a budget nearly double in size over five years.
- CISA has improved public-private integration efforts, mostly through the Joint Cyber Defense Collaborative (JCDC).
- The State Department's Bureau of Cyberspace and Digital Policy (CDP), under its inaugural leader, Ambassador-at-Large Nathaniel Fick, has advanced U.S. interests through cyber diplomacy and cyber capacity building for allies and partners.
- CDP published the first U.S. International Cyberspace and Digital Policy Strategy in May 2024.

On the legislative front, Congress has strengthened the foundations of cybersecurity in the private sector and within federal agencies. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) mandates that critical infrastructure entities report significant cyber incidents to CISA. CISA is now in the final rulemaking process to implement congressional intent.

Congress has also provided the executive branch with increased resources to address cybersecurity challenges facing the federal government, the U.S. military, and the private sector. The fiscal year (FY) 2024 omnibus spending bill, for example, appropriated a much-needed $2.8 billion for CISA and $22 million for the ONCD. The funding for sector risk management agencies, however, has been inconsistent, reflecting a failure of some federal agencies to recognize their responsibilities and request appropriate funding to support interagency efforts and collaborate with critical infrastructure owners and operators. To improve coordination and address funding disparities, in July 2024, the ONCD and the Office of Management and Budget (OMB) issued a joint memorandum outlining the administration's FY26 cybersecurity priorities to modernize technology, enhance public-private collaboration, combat cybercrime, and strengthen the cyber workforce while preparing for emerging threats and expanding global partnerships.

Progress Toward Implementation of the March 2020 Recommendations



The private sector is indispensable not only in securing its own networks but also in working with the federal government on cybersecurity policy development and implementation. Private sector participation in initiatives like the JCDC and the U.S. Cyber Trust Mark, a voluntary software labeling program for Internet of Things devices, will be key in guiding consumer choices and promoting manufacturer accountability for creating secure products. Additionally, private sector investments are supporting and shaping cybersecurity workforce and education policies, creating a more diverse workforce.

While significant progress has been made, more work needs to be done. Increasing cyber incidents targeting America's critical infrastructure sectors, like water and wastewater, aviation, and space, underscore the need for vigilance and robust defensive measures. This year's assessment includes recommendations of what the next Congress and administration should prioritize.

The Biden administration, Congress, and private sector leaders have followed the path charted by the Cyberspace Solarium Commission to defend U.S. national security and economic prosperity in cyberspace. Collectively, these efforts are improving layered cyber deterrence — a critical national security endeavor. We urge readers to consider this report as a way to gauge America's collective efforts while identifying areas where additional initiatives and deeper partnerships are necessary to improve national cyber resilience.

Angus King

Senator Angus King (I-ME)
Co-Chair
CSC 2.0

Representative Mike Gallagher (R-WI)
Co-Chair
CSC 2.0

Top 10 Recommendations for the Incoming Administration and Congress

1. Designate Benefits and Burdens for Systemically Important Entities (5.1)

Prioritization among various critical infrastructure assets is imperative since the United States cannot protect everything, everywhere, all at once. Through NSM-22, President Biden tasked CISA with working with the other sector risk management agencies to identify systemically important entities (SIEs) within each critical infrastructure sector that have a disproportionate impact on U.S. national security, economic security, and public health and safety. NSM-22, however, does not outline the benefits and burdens for companies identified as SIEs, a key component of the CSC's initial recommendation on systemically important critical infrastructure. The next administration and Congress should work together to detail the intelligence and information-sharing benefits and the minimum cybersecurity burdens of SIEs.

2. Conduct Robust Continuity of the Economy Planning (3.2)

A national Continuity of the Economy (COTE) plan 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 National Defense Authorization Act (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. 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.

3. Codify Joint Collaborative Environment for Threat Information Sharing (5.2)

The joint collaborative environment's (JCE's) advanced integrative platform would facilitate real-time sharing and analysis of cyber threat intelligence among government agencies, private sector entities, and international partners. CISA's JCDC has driven forward the concept of a JCE. However, JCDC planning and coordination efforts typically involve fewer than 20 organizations and require additional legal authorities and a platform like the JCE to scale up its work. Private partners will play a crucial role in feeding information into the JCE, while federal agencies provide the structure for sharing data and analytical insights. The next administration and Congress need to codify JCE into law and ensure sustained funding for it. Once established, the JCE will require data privacy and legal protection measures to safely share intelligence information among participants.

4. Strengthen an Integrated Cyber Center Within CISA (5.3)

Establishing an integrated cyber center (ICC) within CISA is essential to achieving a unified national defense against cyber threats. Currently, national cyber defense capabilities are fragmented across various federal agencies. For example, delays and inefficiencies in the response to the SolarWinds hack in 2020 highlighted the need for improved coordination between agencies like the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and CISA. Similarly, the May 2021 Colonial Pipeline ransomware attack demonstrated the need for a centralized approach to handle such incidents effectively. In addition to centralizing expertise and capabilities within CISA and empowering it as the nation's civilian cyber defense agency, the ICC would serve as a hub, standardizing response mechanisms and reducing redundancy and resource waste. As recommended by the Commission, the ICC would leverage specialized skills and insights from various federal agencies. For instance, the FBI would offer investigative capabilities, the NSA would provide intelligence insights, and CISA could provide its technical and homeland-specific cyber expertise. The ICC can also serve as a focal point for public-private collaboration by building on CISA's existing partnerships and information-sharing channels.

5. Develop Cloud Security Certification (4.5)

The widespread adoption of cloud computing by government agencies and critical infrastructure owners and operators should be a net positive for cybersecurity due to the deeper expertise in network security that cloud service providers can offer. However, recent years have seen dramatic failures by cloud providers to maintain a culture of cybersecurity and include cybersecurity services in their baseline offerings. In these cases, malicious actors have accessed unclassified government networks and critical infrastructure through cloud platforms. Currently, the United States lacks a standardized approach to securing the federal cloud infrastructure. While the FY23 NDAA authorized the Federal Risk and Authorization Management Program (FedRAMP) to standardize security assessment of cloud computing products and services for unclassified federal information, the program does not explicitly enforce cybersecurity standards through a security certification or other mechanisms. In addition to addressing these FedRAMP issues, the government should recognize and designate cloud service providers as a critical infrastructure. This designation, as recommended by the Commission, would either classify cloud services as a stand-alone critical infrastructure sector or, at least, as a unique sub-sector within the information technology sector. Appointing a sector risk management agency for oversight and management of cloud service providers can further mitigate risks.

6. Establish a Bureau of Cyber Statistics (4.3)

Currently, policymakers rely on outdated, incomplete, and inaccurate data on cybersecurity to make strategic decisions. In its March 2020 report, the Commission recommended establishing a Bureau of Cyber Statistics to serve as the federal statistical agency for collecting, analyzing, and disseminating cybersecurity data. The next administration should work with Congress to establish this bureau, ensuring it adheres to the standards and requirements set forth by the existing national statistical agencies and enables the secure curation of holistic data reflective of today's cybersecurity landscape. The Bureau could initially utilize data from federal agencies, such as data collected by CISA as mandated by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Additionally, the sector-based risk assessments required by NSM-22 would further support access to standardized data. Coordination with academia and the private sector would also facilitate the sharing of insights and best practices, enhancing the bureau's ability to inform cybersecurity strategies.

7. Establish Liability for Final Goods Assemblers (4.2)

Establishing liability for final goods assemblers will hold manufacturers accountable for cybersecurity breaches that exploit vulnerabilities in their products, incentivizing them to develop products that are secure from the outset. The liability framework would not only enhance product security but also ensure industry-wide improvements by requiring manufacturers to conduct thorough security testing before products reach consumers. While the ONCD has begun efforts to develop a flexible software liability framework, the effort is still nascent. Meanwhile, in a complementary effort, the Federal Communications Commission has finalized rules for its voluntary labeling program for consumer Internet of Things devices, known as the U.S. Cyber Trust Mark program. However, implementing liability requirements will require legislative action and a flexible regulatory framework. These should define manufacturers' responsibilities, conditions for liability, and penalties for non-compliance. Establishing these frameworks will promote transparency, accountability, and a culture of security across the technology industry, ultimately bolstering national security.

8. Develop Cybersecurity Insurance Certifications (4.4)

The current cyber insurance market is volatile, and too few companies have the coverage they need at premiums they can afford. In June 2024, Kimberly Denbow, vice president of the American Gas Association, warned that gas utilities are struggling with a limited “number of insurance providers willing to write cyber insurance policies.” Four years ago, the Commission recommended that the Department of Homeland Security fund a federally funded research and development center (FFRDC) to research the insurance industry and help insurers find ways to offer better coverage that meets various sector-specific needs. Congress and the Biden administration have done little on this front even as the need for such an FFRDC has only grown. As originally envisioned by the Commission, the FFRDC would also work with the private sector and state insurance regulators to develop certification frameworks for cybersecurity insurance products as well as cyber insurance-related training models for underwriters and claims adjusters.

9. Establish National Guard Cybersecurity Roles (3.3.6)

The National Guard’s unique position bridging the military and civilian sectors, as well as federal and state government authorities, makes it ideally suited to respond to domestic cyber threats. The 54 Guard entities have the local presence and capabilities that position them well to serve as a rapid response force for cyber incidents at both the state and federal levels. Over the years, the Guard has taken on more cybersecurity responsibilities and built more cyber capacity with specialized training and initiatives like the annual Cyber Shield exercise. Additionally, the Guard has participated in numerous state-level cybersecurity efforts. Building increased interoperability between CISA and the Guard could drastically improve the nation’s speed and agility in responding to cyberattacks. However, increasing the cybersecurity response planning responsibilities of the Guard would require multiple facilitating actions from the incoming administration and Congress. Congress should assess how to integrate the Guard more effectively into executive branch cyber response planning efforts like the Department of Homeland Security’s National Cyber Incident Response Plan (NCIRP) and state governor-directed cyber response and recovery operations. To achieve this integration, the next administration and Congress need to determine the Guard’s long-term role in the cyber protection of critical infrastructures and identify the necessary authorities and resources to do this. It is also critical to issue guidance detailing the Guard’s responsibilities, as well as those of CISA and the FBI, in collaboration efforts during incidents.

10. Build Societal Resilience Against Cyber-Enabled Information Operations (3.5)

Cyber-enabled malign influence operation campaigns pose a significant threat to the United States by undermining democratic processes, eroding public trust, and exacerbating social divisions. Enhancing public awareness through digital literacy educational programs is crucial for all age groups in countering these malign efforts. This year, several grants funded through the American Rescue Plan Act of 2021 and the bipartisan Infrastructure Investment and Jobs Act of 2021 have created digital literacy programs at the state level. While these programs are a step forward, the Commission recommends that Congress task the Department of Education, Department of Homeland Security, National Science Foundation, and the National Institute of Standards and Technology with developing curriculums focused on critical thinking and fact-checking skills, equipping citizens to identify disinformation and foreign influence. A successful curriculum would integrate social media literacy into K-12 lesson plans and promote adult education programs on digital citizenship. Investments in civic education are also essential. The next administration should request and Congress should appropriate increased funding for civic education to support these efforts to counter foreign malign influence operations.

Timeline

September 2023

- The Department of Defense releases an unclassified summary of its 2023 Cyber Strategy

October 2023

- President Biden issues Executive Order 14110 on the safe, secure, and trustworthy development and use of artificial intelligence
- The Biden administration announces 31 Regional Innovation and Technology Hubs across the United States

December 2023

- Congress passes the FY24 NDAA with various cybersecurity provisions, including a pilot program on Continuity of the Economy at military bases, cybersecurity enhancements for nuclear command, control, and communications network, and the establishment of a cyber assistance fund at the State Department
- The Department of Health and Human Services releases a concept paper outlining the Department's cybersecurity strategy for the healthcare and public health sector
- Senate confirms Harry Coker Jr. as the new national cyber director

February 2024

- The Biden administration announces an initiative to bolster the cybersecurity of U.S. ports
- President Biden issues Executive Order 14117 to protect Americans' sensitive personal data from exploitation by countries of concern

March 2024

- President Biden issues Executive Order 14119 on expanding registered apprenticeships and promoting labor-management forums
- The Federal Communications Commission approves the U.S. Cyber Trust Mark
- The Department of Defense releases its first Investment Strategy
- Congress provides the first appropriations for the State Department's cyber assistance fund as part of the consolidated appropriations bill

April 2024

- President Biden signs National Security Memorandum 22 on Critical Infrastructure Security and Resilience

May 2024

- The Bureau of Cyberspace and Digital Policy publishes the first U.S. International Cyberspace and Digital Policy Strategy
- The White House releases the second National Cybersecurity Strategy Implementation Plan and the inaugural National Cyber Posture Review

June 2024

- The White House releases a progress report on the National Cybersecurity Workforce and Education Strategy

July 2024

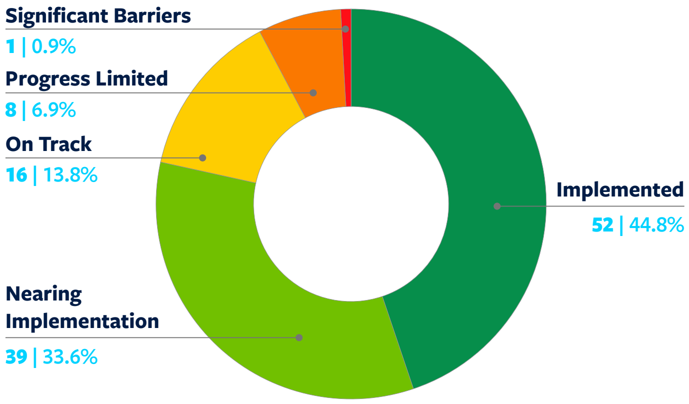
- The Office of Management and Budget and the Office of the National Cyber Director release a memorandum on the administration's cybersecurity priorities for the FY26 budget
- The NATO allies pledge to establish new minimum cybersecurity practices

Evaluating Progress

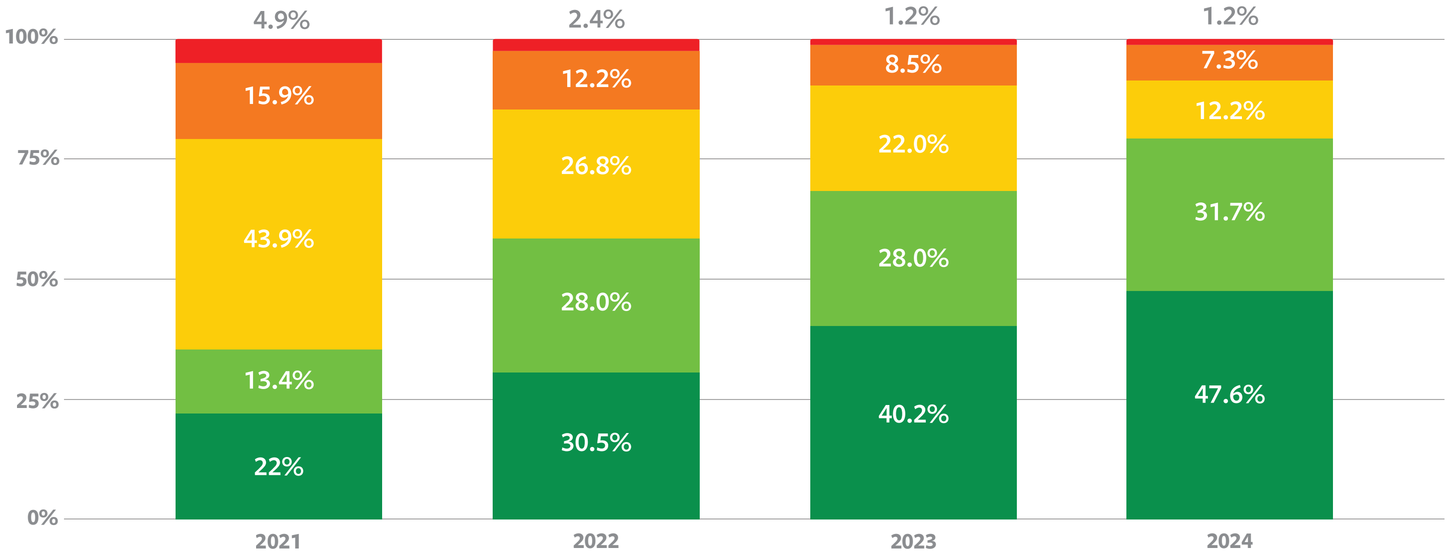
The FY21 NDAA added to the CSC's original mandate by including the charge to review the implementation of the CSC's recommendations and provide annual updates.[2] This report is the fourth annual implementation review responding to that mandate.

Congress created the U.S. Cyberspace Solarium Commission to identify a strategic approach to securing cyberspace. The CSC 2.0 project has continued this mission, assessing and advocating for the Commission's work. This annual assessment report shows that of the Commission's 116 recommendations, including those in their March 2020 report and subsequent white papers, more than three quarters are fully implemented or nearing implementation.

Progress Toward Implementation of All 116 Recommendations



The CSC's March 2020 report separated its original 82 recommendations into six thematic pillars. The following section proceeds by pillar and then turns to the subsequent white papers the Commission issued to address emerging issues and add greater detail to existing recommendations.



🟩 **Implemented:** Legislation has been passed, an executive order issued, or other definitive action taken.

🟩 **Nearing Implementation/Partial Implementation:** The recommendation is included in legislation or an executive order that has a clear path to approval, or it is partially implemented in law/policy.

🟨 **On Track:** The recommendation is being considered for a legislative vehicle, an executive order or other policy is being considered, or there are measurable/reported signs of progress.

🟧 **Progress Limited/Delayed:** The recommendation has not been rejected, but it is not in a legislative vehicle, and there are no known policy actions underway.

🟥 **Significant Barriers to Implementation:** These recommendations are not expected to move in the immediate future but are ready to be taken up if future crises spur action.

Recommendations From the March 2020 CSC Report

The CSC's March 2020 report presented 82 recommendations separated into six thematic pillars. Proceeding by pillar, this section outlines progress on each recommendation.

Pillar 1: Reform the U.S. Government's Structure and Organization for Cyberspace

Reform the U.S. Government's Structure and Organization for Cyberspace					
Rec. Number	Recommendation Title	2021	2022	2023	2024
1.1	Issue an Updated National Cyber Strategy	🟢	🟢	🟩	🟩
1.1.1	Develop a Multitiered Signaling Strategy	🟨	🟨	🟩	🟩
1.1.2	Promulgate a New Declaratory Policy	🟧	🟨	🟩	🟩
1.2	Create House Permanent Select and Senate Select Committees on Cybersecurity	🟥	🟥	🟥	🟥
1.2.1	Re-establish the Office of Technology Assessment	🟨	🟨	🟨	🟧
1.3	Establish National Cyber Director Position	🟩	🟩	🟩	🟩
1.4	Strengthen the Cybersecurity and Infrastructure Security Agency	🟩	🟩	🟩	🟩
1.4.1	Codify and Strengthen the Cyber Threat Intelligence Integration Center	🟧	🟢	🟢	🟩
1.4.2	Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force	🟨	🟢	🟩	🟩
1.5	Diversify and Strengthen the Federal Cyberspace Workforce	🟨	🟢	🟩	🟩
1.5.1	Improve Cyber-Oriented Education	🟩	🟩	🟩	🟩

🟩 **1.1 – Issue an Updated National Cyber Strategy**: *Fully implemented via executive action.* On March 2, 2023, the Biden administration issued the National Cybersecurity Strategy,[3] fully implementing this recommendation. In May 2024, the administration published the second version of its National Cybersecurity Strategy Implementation Plan[4] and the 2024 cyber posture report.[5] The second implementation plan noted that the administration had completed 33 initiatives aimed at implementing the strategy and introduced 31 new initiatives.[6]

🟩 **1.1.1 – Develop a Multitiered Signaling Strategy**: *Fully implemented via executive action.* The National Cybersecurity Strategy publicly communicates U.S. goals and intent in cyberspace, including the administration's willingness to use both cyber and non-cyber tools to push back on U.S. adversaries.

🟩 **1.1.2 – Promulgate a New Declaratory Policy**: *Fully implemented via executive and legislative actions*. The publication of the National Cybersecurity Strategy serves as a declaratory policy vital for deterrence against adversaries, fully implementing this recommendation.[7] In 2024, the new U.S. International Cyberspace and Digital Policy Strategy further promotes secure digital ecosystems and responsible behavior in cyberspace.[8]

🟥 **1.2 – Create House Permanent Select and Senate Select Committees on Cybersecurity**: *Faces significant barriers to implementation; further executive and legislative actions required.* Significant pushback against this recommendation continues into the fourth year. Prior to the end of the Commission's tenure, staff drafted legislative language should a future emergency create the political impetus to overcome existing barriers.

🟧 **1.2.1 – Re-establish the Office of Technology Assessment**: *Progress limited/delayed; further appropriations required.* As noted in previous annual assessments, Congress indicated it intends to increase funding for the Government Accountability Office (GAO) and Congressional Research Service (CRS) rather than re-establish the Office of Technology Assessment. The Supreme Court's ruling overturning a principle known as the Chevron doctrine, which had provided federal agencies the ability to interpret ambiguous or broad statutes, will likely drive an increased demand signal from congressional members and professional and personal staff for technical support on cybersecurity issues.[9] In the president's FY25 budget, GAO requested a 12.8 percent increase over FY24 enacted levels to fund work in science, technology, cybersecurity, and other issues.[10] While CRS also requested a 7 percent increase,[11] it remains understaffed in its cybersecurity mission, limiting its ability to provide comprehensive analysis. It is crucial that Congress approves these funding levels to ensure GAO and CRS can provide essential nonpartisan analysis to fill the gap left by the defunct Office of Technology Assessment.

🟩 **1.3 – Establish a National Cyber Director Position**: *Fully implemented via executive and legislative action.* The Senate confirmed Harry Coker, Jr. on December 12, 2023, as the second national cyber director, succeeding Chris Inglis.[12] Coker brings a wealth of experience from his previous roles as a senior executive at the CIA and as executive director of the NSA.[13]

🟩 **1.4 – Strengthen the Cybersecurity and Infrastructure Security Agency**: *Fully implemented via legislative action and appropriations; further appropriations required*. The FY24 omnibus spending bill appropriated CISA $2.8 billion, $35 million less than FY23 enacted levels. This year, the president's budget requested $180 million above the previous enacted level.[14] In her testimony before the House Appropriations Committee, CISA Director Jen Easterly highlighted three key areas of CISA's investment: 1) federal network cybersecurity, 2) critical infrastructure protection, and 3) threat hunting and mitigation. Consistent investments over the years have allowed CISA to remediate over 25 million unpatched vulnerabilities, expand field presence by 35 percent, and deploy endpoint detection tools to over 50 agencies, covering 900,000 devices.[15] In April 2024, President Biden signed NSM-22, codifying CISA as the National Coordinator to oversee federal national risk management efforts.[16]

🟩 **1.4.1 – Codify and Strengthen the Cyber Threat Intelligence Integration Center**: *Fully implemented via legislative action and appropriations.* The Biden administration re-established the Cyber Threat Intelligence Integration Center (CTIIC) at the Office of the Director of National Intelligence in FY22.[17] With increased budget and manpower, CTIIC will play a critical role in integrating and disseminating cyber threat intelligence across federal agencies and supporting the director of national intelligence as the federal lead for intelligence support, as named in NSM-22.[18] CTIIC will also play a lead role as a federal integrator in cyber open-source intelligence collaboration.

🟩 **1.4.2 – Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force**: *Fully implemented via appropriations.* In 2023, the FBI took over 1,000 actions against cyber adversaries, issued thousands of "individualized threat warnings," and disseminated 78 public threat advisories.[19] This year, the president's budget includes a total of $11.3 billion for the FBI, with $7 million dedicated to enhancing cyber investigative capabilities.[20] Additionally, the FBI expanded its network of Cyber Assistant Legal Attachés from 16 to 22 to further enhance global cyber threat intelligence and response capabilities.[21]

🟩 **1.5 – Diversify and Strengthen the Federal Cyberspace Workforce**: *Fully implemented via legislative actions and increased appropriations*. Following the release last year of the National Cyber Workforce and Education Strategy, the administration continues to focus on better recruiting and retaining a diverse federal cyber workforce this year. In February 2024, the Office of Personnel Management released a workforce playbook consolidating existing government programs on federal employment, including cybersecurity, to help federal employers utilize the existing resources for fostering an inclusive workforce.[22] Furthermore, many federal entities awarded grants for this effort, including $3.6 million for talent development partnerships at the National Institute of Standards and Technology,[23] $39 million for state, local, tribal, and territorial governments to increase access to cyber education for "women, people of color, individuals with disabilities and underserved communities" through the Department of Labor,[24] and $3 million for training underserved communities through CISA appropriations.[25]

🟩 **1.5.1 – Improve Cyber-Oriented Education**: *Fully implemented via executive actions and appropriations.* CISA's Cybersecurity Education and Training program continues to develop and execute cybersecurity awareness training and education programs for K-12 teachers across the country. The program received $6.8 million for cyber awareness training programs in both FY23 and FY24.[26]

Pillar 2: Strengthen Norms and Non-military Tools

Strengthen Norms and Non-military Tools					
Rec. Number	Recommendation Title	2021	2022	2023	2024
2.1	Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State	🟢	🟩	🟩	🟩
2.1.1	Strengthen Norms of Responsible State Behavior in Cyberspace	🟨	🟢	🟩	🟩
2.1.2	Engage Actively and Effectively in Forums Setting International ICT Standards	🟨	🟢	🟢	🟩
2.1.3	Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance	🟨	🟨	🟢	🟩
2.1.4	Improve International Tools for Law Enforcement Activities in Cyberspace	🟢	🟩	🟩	🟩
2.1.5	Leverage Sanctions and Trade Enforcement Actions	🟧	🟢	🟢	🟢
2.1.6	Improve Attribution Analysis and the Attribution-Decision Rubric	🟧	🟢	🟢	🟢
2.1.7	Reinvigorate Efforts to Develop Cyber Confidence-Building Measures	🟨	🟨	🟨	🟢

🟩 **2.1 – Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State**: *Fully implemented via executive and legislative actions*. The Biden administration established the Bureau of Cyberspace and Digital Policy at the State Department in April 2022, and Congress codified it into law with the passage of the Cyber Diplomacy Act as part of the FY23 NDAA.[27] The Senate-confirmed ambassador-at-large for cyber, Nathaniel Fick, has effectively been leading the bureau for nearly two years.[28] CDP led the drafting of the new U.S. International Cyberspace and Digital Policy Strategy released in May.[29]

🟩 **2.1.1 – Strengthen Norms of Responsible State Behavior in Cyberspace**: *Fully implemented via executive action.* A January 2024 GAO report noted that the elevation of the State Department's Bureau of Cyberspace and Digital Policy to a bureau-level entity has "strengthened cyber issues within the State Department."[30] The bureau has also been instrumental in fostering international cooperation on cybersecurity. In June 2024, for example, CDP hosted discussions with 22 countries and the European Union on growing cybersecurity challenges and "efforts to deter malicious cyber activity and coordinate international responses." Led by Deputy Assistant Secretary Liesyl Franz, these discussions emphasized the importance of strengthening norms and responsibilities, specifically in upholding the UN Framework for Responsible State Behavior in Cyberspace.[31] In the past year, the CDP has been active in several key international forums that have resulted in enhanced international cooperation and collaboration. For example, the U.S.-EU Summit in October 2023 led to the development of best practices for Internet of Things security, known as the CyberSafe Products Action Plan.[32]

🟩 **2.1.2 – Engage Actively and Effectively in Forums Setting International ICT Standards**: *Fully implemented via executive action.* In February 2024, the United States, along with nine international allies and partners, produced a joint statement endorsing shared principles for the research and development of 6G wireless communication systems.[33] Similarly, in April 2024, the U.S.-EU Trade and Technology Council's joint statement committed the parties to "creating rules of the road for emerging technologies" for artificial intelligence and 6G wireless communication by hosting dialogues and information exchange.[34] The Department of Energy, meanwhile, secured commitments from G7 countries and global energy industrial control systems manufacturers to adhere to voluntary supply chain cybersecurity standards.[35] Other agencies, such as the National Telecommunications and Information Administration, are promoting multi-stakeholder engagements at international forums.[36]

🟩 **2.1.3 – Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance**: *Fully implemented via executive and legislative actions and appropriations.* The State Department's Bureau of Cyberspace and Digital Policy has actively promoted cyber capacity-building measures and fostered regional cooperation with specific programs like the Digital Connectivity and Cybersecurity Partnership.[37] Strengthening "partner digital and cyber capacity" was one of four areas of action within the international cyber strategy.[38] Importantly, the FY24 NDAA created a cyber assistance fund — the State Department's Digital Connectivity and Related Technologies Fund — to help partners and allies improve resilience and respond to cyber incidents.[39] Congress appropriated the first $50 million for the fund in the FY24 omnibus spending bill,[40] and House appropriators included another $50 million in the FY25 State and Foreign Operations Appropriations bill.[41] While this dedicated State Department funding is important, the executive branch will need to better integrate interagency partner capacity building efforts.

The FBI's Cyber Assistant Legal Attachés facilitate real-time information sharing and coordinated responses to cyber threats, proving essential in supporting the Department of Justice's focus on combating cybercrimes. Although talks of significant budget cuts raised concerns last year, the program's continued growth demonstrates a commitment to international cyber cooperation.

🟩 **2.1.4 – Improve International Tools for Law Enforcement Activities in Cyberspace**: *Fully implemented via executive action and appropriations.* The FBI's Cyber Assistant Legal Attachés (ALATs) program expanded its reach over the past year, adding six new positions in cities including Brasília, New Delhi, and Rome, increasing the total number of cyber ALATs from 16 to 22.[42] According to the FBI Cyber Division's assistant director, Bryan Vorndran, the FBI can put a "cyber-trained FBI agent on nearly any doorstep in this country within one hour" and accomplish the same feat "in more than 70 countries in one day" thanks to the FBI's network of legal attachés.[43] The ALATs' presence facilitates real-time information sharing and coordinated responses to cyber threats, proving essential in supporting the Department of Justice's focus on combating cybercrimes. Although talks of significant budget cuts raised concerns last year,[44] the program's continued growth demonstrates a commitment to international cyber cooperation.

🟩 **2.1.5 – Leverage Sanctions and Trade Enforcement Actions**: *Nearing/partial implementation; further legislative action required.* Little progress has been made in codifying Executive Order 13848, which responds to foreign interference in the United States.[45] However, President Biden extended the authorities under the executive order to September 2024, the second extension since it was originally set to expire in 2022.[46] In 2023 and 2024, the Treasury sanctioned malicious cyber actors and entities from Russia, Iran, and Venezuela.[47] The State Department's Rewards for Justice program, meanwhile, offered rewards of up to $10 million for information leading to the "identification and location" of these cyber criminals.[48]

🟩 **2.1.6 – Improve Attribution Analysis and the Attribution-Decision Rubric**: *Nearing/partial implementation; further executive action required.* Since the May 2023 Cybersecurity Advisory on the Chinese state-sponsored malicious actor Volt Typhoon,[49] CISA, the FBI, the NSA, and other federal agencies have continued to warn about the threat from this group and provide vital guidance to U.S. critical infrastructure owners and operators.[50] Washington has also continued to emphasize joint attribution of malicious activity.[51] The 2024 cyber posture report stresses that part of federal efforts to provide "support to victims" includes "employing a global network of cyber threat experts contributing to attribution and analysis."[52]

🟩 **2.1.7 – Reinvigorate Efforts to Develop Cyber Confidence-Building Measures**: *Nearing/partial implementation; further executive action required.* The Bureau of Cyberspace and Digital Policy is leading discussions bilaterally, in the United Nations Group of Governmental Experts and Open-Ended Working Group, and in regional fora to articulate norms of responsible behavior as well as confidence-building measures.[53] The bureau's prioritization of cyber confidence-building measures aimed at increasing trust and cooperation between nations should continue.

Pillar 3: Promote National Resilience

Promote National Resilience					
Rec. Number	Recommendation Title	2021	2022	2023	2024
3.1	Codify Sector-Specific Agencies as Sector Risk Management Agencies and Strengthen Their Ability to Manage Critical Infrastructure Risk	🟩	🟩	🟩	🟩
3.1.1	Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy	🟢	🟨	🟨	🟩
3.1.2	Establish a National Cybersecurity Assistance Fund	🟨	🟧	🟨	🟨
3.2	Develop and Maintain Continuity of the Economy Planning	🟩	🟢	🟢	🟢
3.3	Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"	🟢	🟩	🟩	🟩
3.3.1	Designate Responsibilities for Cybersecurity Services Under the Defense Production Act	🟥	🟢	🟢	🟢
3.3.2	Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts	🟧	🟧	🟧	🟧
3.3.3	Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts	🟨	🟨	🟢	🟢
3.3.4	Expand Coordinated Cyber Exercises, Gaming, and Simulation	🟩	🟩	🟩	🟩
3.3.5	Establish a Biennial National Cyber Tabletop Exercise	🟩	🟩	🟩	🟩
3.3.6	Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard	🟩	🟢	🟨	🟨
3.4	Improve the Structure and Enhance Funding of the Election Assistance Commission	🟨	🟢	🟢	🟢
3.4.1	Modernize Campaign Regulations to Promote Cybersecurity	🟨	🟧	🟧	🟧
3.5	Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations	🟧	🟧	🟨	🟨
3.5.1	Reform Online Political Advertising to Defend Against Foreign Influence in Elections	🟨	🟨	🟨	🟨

🟩 **3.1 – Codify Sector-Specific Agencies Into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk**: *Fully implemented via legislative action.* Congress codified sector risk management agencies (SRMAs) in law through the FY21 NDAA,[54] fully implementing this recommendation. In April 2024, the White House issued a new National Security Memorandum on Critical Infrastructure Security and Resilience, NSM-22, codifying CISA as the National Coordinator responsible for working with other SRMAs to fulfill their responsibilities and identifying cross-sector risks.[55] While this memorandum provides much-needed reaffirmation of SRMA duties, appropriators also need to ensure that SRMAs receive adequate funding to be successful.

🟩 **3.1.1 – Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy**: *Fully implemented via executive action.* NSM-22 fully implemented this recommendation by directing the Department of Homeland Security, through CISA, to create a coordinated national risk management cycle to "identify, assess, and prioritize [cyber and physical] risk" facing critical infrastructure. This includes developing sector-specific risk assessments and risk management plans that will be integrated into a biennial National Infrastructure Risk Management Plan.[56]

🟨 **3.1.2 – Establish a National Cybersecurity Assistance Fund**: *On track; awaiting legislative action.* Various legislative actions and sector-specific grant programs align with the intent of this recommendation,[57] but a National Cybersecurity Assistance Fund would address systemic cyber risks over a longer period of time.

🟩 **3.2 – Develop and Maintain Continuity of the Economy Planning**: *Nearing/partial implementation via legislation; further executive action required*. Last year, the Biden administration belatedly submitted its Continuity of the Economy plan to Congress as mandated by the FY21 NDAA.[58] The report, however, determined that existing government incident response and emergency management planning was sufficient, dismissing congressional concerns that prompted the NDAA provision in the first place. The White House (National Security Council) report brushed aside gaps in current federal incident response capabilities and failed to grapple with the ways the private sector must be involved in the development and implementation of the plan.

🟩 **3.3 – Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"**: *Fully implemented via legislative action and appropriations.* Provisions in the Infrastructure Investment and Jobs Act of 2021 implemented this recommendation.[59]

🟩 **3.3.1 – Designate Responsibilities for Cybersecurity Services Under the Defense Production Act**: *Nearing/partial implementation via executive action.* The Department of Defense (DoD) can utilize the Defense Production Act to accelerate the procurement of critical cybersecurity technologies and allow modifications to acquisition requirements. The DoD's 2023 National Defense Industrial Strategy focuses on strengthening the Defense Industrial Base (DIB) posture to support defense operations. The strategy aligns with the intent of this recommendation, specifically, its acknowledgment that DoD can use the Defense Production Act and other programs to offset cybersecurity costs and thereby enable small and non-traditional businesses "that improve DoD's technology edge and capabilities" to participate in the DIB.[60] Further executive action is required to include cybersecurity services as part of the broader strategy to secure critical infrastructure.

🟧 **3.3.2 – Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts**: *Progress limited; further legislative action required.* While the Commission staff drafted legislation in support of this recommendation, no comprehensive policy has been established insulating companies from liability if they take cyber and emergency response actions directed by the federal government or law enforcement.

🟩 **3.3.3 – Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts**: *Nearing/partial implementation via executive action; further legislative action required.* CISA is updating and expected to release the National Cyber Incident Response Plan for significant incident response coordination by the end of the year.[61] The plan should incorporate two elements: 1) outlining how federal, state, local, tribal, and territorial governments and private entities respond to significant cyber incidents affecting critical infrastructure, and 2) identifying options and resources to supplement the government's response. Integrating the two into existing emergency response and disaster recovery mechanisms is crucial.

🟩 **3.3.4 – Expand Coordinated Cyber Exercises, Gaming, and Simulation**: *Fully implemented via legislative action and appropriations.* The FY22 NDAA implemented this recommendation.[62] The president's FY25 budget, however, requests $12.6 million less for the National Infrastructure Simulation Analysis Center than in the previous year,[63] potentially limiting the center's capacity to conduct essential cyber exercises and readiness simulations.

🟩 **3.3.5 – Establish a Biennial National Cyber Tabletop Exercise**: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation, ensuring regular cyber preparedness drills for critical infrastructure.[64]

🟨 **3.3.6 – Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard**: *On track; pending report to Congress.* According to National Guard officials, the Guard has more than 2,000 soldiers trained in cybersecurity.[65] The National Guard's unique position bridging military and civilian sectors and federal and state government authorities makes it ideally suited to respond to domestic cyber threats. Additionally, the Guard also plays a role in international cyber capacity building. From June 24 to July 5, 2024, approximately 50 guardsmen and airmen participated in the Adriatic Regional Security Cyber Cooperation in Slovenia alongside servicemembers from seven other countries. Earlier in the year, nearly 1,000 participants, many of whom are members of the National Guard State Partnership Program, gathered in Virginia for Cyber Shield 2024, a two-week cybersecurity training hosted by the National Guard. This event is the "longest-running and largest Department of Defense cyber defense exercise," according to the department.[66]

🟩 **3.4 – Improve the Structure and Enhance Funding of the Election Assistance Commission**: *On track; further appropriations required.* Over the past two fiscal years, Congress appropriated about $28 million annually for the Election Assistance Commission (EAC) and also provided the EAC with an additional $75 million per year for election security grant funding as established by the Help America Vote Act. These levels are appropriate; however, earlier this year, House appropriators recommended a significant reduction.[67] The House version of the annual appropriations bill rejected the EAC's request for $96 million for election security grants and reduced the EAC's base funding to $20 million, back to the level the EAC received in FY22.[68] The Senate appropriators, however, included $75 million for election security grant funding in the Senate version ahead of the committee markup.[69] Appropriators must recognize that the reductions, particularly the rejection of funding for security grants, are significant cybersecurity setbacks.

> ***Over the past two fiscal years, Congress appropriated about $28 million annually for the Election Assistance Commission (EAC) and also provided the EAC with an additional $75 million per year for election security grant funding as established by the Help America Vote Act. These levels are appropriate.***

🟧 **3.4.1 – Modernize Campaign Regulations to Promote Cybersecurity**: *Progress limited; further legislative action required.* In April 2024, the Federal Election Commission proposed amendments to clarify how federal candidates can use campaign funds for cybersecurity measures.[70] This proposal, however, is still under review months ahead of the 2024 presidential and congressional elections. While CISA and nonprofits can provide services, there has been limited progress in amending the Federal Election Campaign Law to allow corporations to provide free or reduced-cost cybersecurity assistance to political campaigns on a nonpartisan basis.

🟨 **3.5 – Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations**: *On track via executive action; further executive action and appropriations required.* Progress has remained steady with state-level digital literacy efforts spurred by the American Rescue Plan Act of 2021 and the bipartisan Infrastructure Investment and Jobs Act of 2021.[71] For instance, in February 2024, Kansas announced a $2.8 million award to 15 organizations to provide digital literacy training programs.[72] And in April 2024, California received a $70 million award to implement measures in the "California Digital Plan" to provide affordable internet and digital literacy education to its state residents.[73] Despite these efforts, further executive action and appropriations are required to build societal resilience.

🟨 **3.5.1 – Reform Online Political Advertising to Defend Against Foreign Influence in Elections**: *On track via appropriations; further legislative action required.* On February 14, 2024, the Election Assistance Commission unanimously approved the use of election security grant funds "to counter disinformation generated through the use of artificial intelligence."[74] This funding will go toward voter education and promoting accurate voting procedures to counteract disinformation. FBI Director Christopher Wray noted the urgency of foreign influence in U.S. elections, warning that adversaries are "moving at a faster pace, and enabled by new technology."[75] In January 2024, days before his retirement, then-U.S. Cyber Command General Paul Nakasone voiced his confidence in election security, stating that the upcoming election "will be the most secure election we've had to date."[76] There still remains a need to extend and apply traditional media's political advertising standards and limitations to social media.

Pillar 4: Reshape the Cyber Ecosystem Toward Greater Security

Reshape the Cyber Ecosystem toward Greater Security					
Rec. Number	Recommendation Title	2021	2022	2023	2024
4.1	Establish and Fund a National Cybersecurity Certification and Labeling Authority	🟨	🟨	🟩	🟢
4.1.1	Create or Designate Critical Technology Security Centers	🟨	🟩	🟩	🟩
4.1.2	Expand and Support the National Institute of Standards and Technology Security Work	🟧	🟢	🟢	🟩
4.2	Establish Liability for Final Goods Assemblers	🟥	🟥	🟧	🟩
4.2.1	Incentivize Timely Patch Implementation	🟨	🟨	🟩	🟨
4.3	Establish a Bureau of Cyber Statistics	🟨	🟧	🟨	🟨
4.4	Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications	🟨	🟧	🟧	🟨
4.4.1	Establish a Public-Private Partnership on Modeling Cyber Risk	🟨	🟨	🟨	🟨
4.4.2	Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events	🟨	🟨	🟩	🟩
4.4.3	Incentivize Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities	🟢	🟢	🟢	🟢
4.4.4	Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements	🟨	🟨	🟢	🟢
4.5	Develop a Cloud Security Certification	🟨	🟨	🟩	🟩
4.5.1	Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments	🟨	🟩	🟩	🟩
4.5.2	Develop a Strategy to Secure Foundational Internet Protocols and Email	🟩	🟩	🟩	🟩
4.5.3	Strengthen the U.S. Government's Ability to Take Down Botnets	🟨	🟨	🟨	🟩
4.6	Develop and Implement an ICT Industrial Base Strategy	🟩	🟩	🟩	🟩
4.6.1	Increase Support to Supply Chain Risk Management Efforts	🟨	🟢	🟢	🟢
4.6.2	Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies	🟨	🟢	🟢	🟢
4.6.3	Strengthen the Capacity of the Committee on Foreign Investment in the United States	🟧	🟩	🟩	🟩
4.6.4	Invest in the National Cyber Moonshot Initiative	🟨	🟩	🟩	🟩
4.7	Pass a National Data Security and Privacy Protection Law	🟥	🟨	🟨	🟧
4.7.1	Pass a National Breach Notification Law	🟨	🟧	🟧	🟧

🟩 **4.1 – Establish and Fund a National Cybersecurity Certification and Labeling Authority**: *Fully implemented via executive action.* The Federal Communications Commission in March approved the U.S. Cyber Trust Mark, a voluntary cybersecurity labeling program for consumer Internet of Things devices,[77] fully implementing this recommendation. This initiative certifies devices that meet cybersecurity criteria outlined by the National Institute of Standards and Technology,[78] helping consumers make informed decisions and encouraging manufacturers to adopt secure practices. Major retailers and technology companies, including Amazon, BestBuy, and Google, have signed up to participate.[79]

🟩 **4.1.1 – Create or Designate Critical Technology Security Centers**: *Nearing/partial implementation via legislative action; further legislative action required.* This recommendation was partially implemented through appropriations from the Infrastructure Investment and Jobs Act to the Department of Homeland Security's Science and Technology Directorate.[80] Additionally, last year, Rep. Ritchie Torres (D-NY) introduced the Critical Technology Security Centers Act of 2023 to establish and fund two centers for testing critical device security and developing mitigation measures, but it has seen no movement in Congress.[81]

🟩 **4.1.2 – Expand and Support the National Institute of Standards and Technology Security Work**: *Nearing/partial implementation via appropriations; further appropriations required.* In February, the National Institute of Standards and Technology (NIST) released the second iteration of its Cybersecurity Framework, a widely used gold standard for measuring cybersecurity.[82] The president's FY25 budget request, however, proposes only $96.8 million for the cybersecurity and privacy program,[83] below the funding levels the Commission recommended four years ago.[84] While NIST's funding has increased since the Commission's March 2020 report, it still remains far below what is necessary given how many new responsibilities Congress and the administration have tasked to NIST.[85] Repeated failures to match funding to tasking leave NIST unable to perform its traditional cybersecurity responsibilities or its new tasking under various executive orders and legislation, which causes our assessment of this recommendation to regress.

🟩 **4.2 – Establish Liability for Final Goods Assemblers**: *Nearing/partial implementation via executive action; further executive and legislative actions required.* The ONCD noted in its National Cybersecurity Strategy Implementation Plan that it will "explore approaches to developing a long-term, flexible, and enduring software liability framework" by the second quarter of FY24.[86] National Cyber Director Harry Coker announced in February 2024 that the ONCD has started efforts to hold software manufacturers that "rush code to market" liable for vulnerabilities in their software.[87] During the May 2024 RSA conference, ONCD Assistant Director for Cyber Policy and Programs Nick Leiserson announced that the White House started its outreach efforts to software manufacturers in March and is set to continue over the next "eight to 10 months."[88]

🟨 **4.2.1 – Incentivize Timely Patch Implementation**: *On track via executive action; further appropriations required.* While last year's assessment report noted that the National Institute of Standards and Technology (NIST) updated its Guide to Enterprise Patch Management Technologies in April 2022, NIST's inability to process new additions to the National Vulnerability Database (NVD) has degraded the ability of public and private sector entities to manage vulnerabilities and risks. In February 2024, NIST temporarily halted adding Common Vulnerabilities and Exposures to its NVD, citing limited capacity to conduct security analysis.[89] As of July, NIST has implemented temporary measures to address the backlog and is seeking to identify an industry consortium to assist with its work.[90] Increased and consistent funding for NIST is critical to rectify this gap.[91]

🟨 **4.3 – Establish a Bureau of Cyber Statistics**: *On track via executive action; further legislative action required.* While Congress has not yet created a Bureau of Cyber Statistics, other developments continue to lay the groundwork for its eventual creation. CISA, for example, is on track to issue a final rule for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), having received industry feedback on its proposed rule.[92] CIRCIA may provide an opportunity to collect data, anonymize it, and disseminate it to a broader audience as intended by the Bureau of Cyber Statistics.[93] The administration and Congress can establish this bureau, ensuring it adheres to the standards and requirements set forth by the existing national statistical agencies and enables the secure curation of data reflective of today's cybersecurity landscape. Additionally, establishing exchange mechanisms with academia and the private sector will facilitate the sharing of insights and best practices, enhancing the bureau's ability to inform cybersecurity strategies.

🟨 **4.4 – Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications**: *On track via legislative action; further executive action required.* The National Science and Technology Council's December 2023 Federal Cybersecurity Research and Development Strategic Plan identifies as a research priority the need to establish "comprehensive frameworks for cybersecurity risk management … by incorporating financial risk mitigations through methods such as cyber insurance."[94] The National Science and Technology Council is a cabinet-level council of advisors to the president. The Commission's original recommendation also includes developing a training and certification program for insurance professionals.

🟨 **4.4.1 – Establish a Public-Private Partnership on Modeling Cyber Risk**: *On track via executive action; further executive action required.* Progress is being made on this recommendation with various public-private partnerships. CISA's Joint Cyber Defense Collaborative released its 2024 priorities, which include raising the national cybersecurity baseline and defending against malicious nation-state actors and emerging risks.[95] Further executive action is required to enhance collective cyber defense.

🟩 **4.4.2 – Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events**: *Nearing/partial implementation via executive action; further executive action required.* The second iteration of the National Cybersecurity Strategy implementation plan noted that Treasury has completed its assessment of the need for a federal cyber insurance backstop.[96] Additionally, Treasury's Federal Insurance Office and the National Science Foundation issued a call for proposals to research insurance risk modeling and underwriting for terrorism and catastrophic cyber risks.[97]

🟩 **4.4.3 – Incentivize Information Technology Security Through Federal Acquisition Regulations and Federal Information Security Management Act Authorities**: *Fully implemented via executive action.* The Biden administration implemented this recommendation in 2021 through Executive Order 14028, "Improving the Nation's Cybersecurity." Passage of the Federal Information Security Modernization Act of 2023[98] would further support this recommendation.

🟩 **4.4.4 – Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements**: *Fully implemented via legislative action.* The Security and Exchange Commission's rules requiring publicly traded companies to disclose material cybersecurity incidents and update cybersecurity risk management policies annually implement this recommendation.[99]

🟩 **4.5 – Develop a Cloud Security Certification**: *Nearing/partial implementation; further executive and legislative actions required.* The Commission urged the National Institute of Standards and Technology and the Department of Homeland Security to develop a standard for attesting to the security of cloud service providers and to update the relevant requirements in the Federal Risk and Authorization Management Program (FedRAMP) so that all cloud providers meet the security standards. FedRAMP's March 2024 roadmap committed to simplifying the process for cloud-based computing infrastructure and applications to become certified to sell to the U.S. government. FedRAMP is also committed to working with CISA to better define security requirements for cloud providers.[100] More executive and legislative action is necessary to expand efforts around securing those cloud services used by the federal government to cover all commercially available cloud service providers.

🟩 **4.5.1 – Incentivize the Uptake of Secure Cloud Services for Small- and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments**: *Nearing/partial implementation via legislative action; further executive and appropriations required.* The State and Local Cybersecurity Improvement Act, passed into law in the bipartisan Infrastructure Investment and Jobs Act, partially implemented this recommendation.[101] In March, the NSA released its "Top Ten Cloud Security Mitigation Strategies," identifying ways for businesses to safely adopt cloud services. This report, however, did not specifically address the needs of small- and medium-sized businesses.[102]

🟩 **4.5.2 – Develop a Strategy to Secure Foundational Internet Protocols and Email**: *Nearing/partial implementation via legislative action; further executive action required.* This recommendation specifically addresses securing three elements: Border Gateway Protocol (BGP), the Domain Name System (DNS), and email communication via the Domain-based Message Authentication, Reporting, and Conformance standard. Previously, the FY21 and FY22 NDAAs addressed parts of this recommendation.[103] Over the past year, the Biden administration has continued to focus on foundational internet protocols. On June 7, 2024, the Federal Communications Commission approved a proposal requiring retail broadband providers to submit confidential reports annually on their BGP security plan and the nine largest providers to submit public reports quarterly.[104] The same month, Acting Principal Deputy National Cyber Director Jake Braun highlighted the government's move to enhance BGP security by adopting Resource Public Key Infrastructure, which verifies the authenticity of internet routing information, making it more difficult for hackers to hijack internet traffic.[105] Additionally, CISA's DNS Resolver blocked 900 million malicious connections targeting federal civilian agencies in FY23.[106]

🟩 **4.5.3 – Strengthen the U.S. Government's Ability to Take Down Botnets**: *Nearing/partial implementation via executive action; further executive action required.* The Department of Justice (DoJ) has enhanced its capabilities to dismantle botnets through various coordinated efforts, fully implementing this recommendation. In January, DoJ led the takedown of the 911 S5 botnet, which FBI Director Christopher Wray described as "likely the world's largest botnet ever."[107] In recent months, DoJ has also dismantled botnets connected with Russian and Chinese government hackers.[108]

🟩 **4.6 – Develop and Implement an ICT Industrial Base Strategy**: *Nearing/partial implementation via executive action; further executive action required.* In December, the Bureau of Industry and Security Office of Technology Evaluation at the Department of Commerce published a report surveying U.S.-based microelectronics companies to better support domestic manufacturing. The report reflected growing concerns over cyberattacks and industry espionage, with 21 percent of respondents expecting challenges from foreign industrial espionage, up from 15 percent in previous years.[109] Previously, the CHIPS and Science Act[110] and other executive action[111] had partially implemented this recommendation. Commerce's new strategy, combined with the Defense Department's National Defense Industrial Strategy, moves the ball forward. Additional executive action is necessary to see these strategies implemented.

🟩 **4.6.1 – Increase Support to Supply Chain Risk Management Efforts**: *Fully implemented via executive and legislative actions.* The February 2021 executive order on supply chain resiliency and the passage of the CHIPS and Science Act fully implemented this recommendation.[112] Supply chain risk management continues to be one of the administration's priorities.[113]

🟩 **4.6.2 – Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies**: *Fully implemented via legislative actions.* The passage of the CHIPS and Science Act fully implemented this recommendation,[114] and Congress has continued to provide consistent funding for emerging technologies research and development.

🟩 **4.6.3 – Strengthen the Capacity of the Committee on Foreign Investment in the United States**: *Nearing/partial implementation via appropriations; further executive action required.* A September 2022 executive order expanded the factors the Committee on Foreign Investment in the United States (CFIUS) uses during its review process.[115] Since then, CFIUS has reviewed an increasing number of transactions each year.[116] Additionally, amid various proposed efforts to improve CFIUS capabilities,[117] the Treasury Department proposed a rule in July to increase scrutiny of foreign investments near military bases by adding 59 military installations to its review list.[118]

🟩 **4.6.4 – Invest in the National Cyber Moonshot Initiative**: *Nearing/partial implementation via legislative action; further appropriations required.* In its report to the president, the National Security Telecommunications Advisory Committee recommended leveraging artificial intelligence and machine learning technologies to improve cybersecurity defenses through various efforts like the launching of Cybersecurity Grand Challenges. The committee also recommended that CISA examine security use cases for emerging technologies.[119] The FY21 NDAA and the CHIPS and Science Act partially implemented this recommendation,[120] but further investment is needed to fully implement it.

🟧 **4.7 – Pass a National Data Security and Privacy Protection Law**: *Progress limited; further legislative action required.* In June 2024, the House of Representatives postponed the scheduled markup of the American Privacy Rights Act, the latest legislative proposal in Congress on data privacy.[121] This third consecutive year of setbacks underscores the ongoing challenges in creating a unified federal data privacy framework.[122]

🟧 **4.7.1 – Pass a National Breach Notification Law**: *Progress limited; further legislative and executive actions required.* Various pieces of legislation require breach notification to consumers under certain circumstances,[123] but comprehensive federal legislation has yet to be enacted.

Pillar 5: Operationalize Cybersecurity Collaboration With the Private Sector

Operationalize Cybersecurity Collaboration With the Private Sector					
Rec. Number	Recommendations Title	2021	2022	2023	2024
5.1	Codify the Concept of "Systemically Important Critical Infrastructure"	🟨	🟨	🟨	🟩
5.1.1	Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector	🟨	🟧	🟨	🟩
5.1.2	Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities	🟨	🟧	🟨	🟩
5.1.3	Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities	🟢	🟢	🟢	🟢
5.2	Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information	🟨	🟨	🟨	🟩
5.2.1	Expand and Standardize Voluntary Threat Detection Programs	🟨	🟢	🟢	🟢
5.2.2	Pass a National Cyber Incident Reporting Law	🟧	🟢	🟢	🟢
5.2.3	Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors	🟨	🟨	🟧	🟧
5.3	Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers	🟢	🟩	🟩	🟩
5.4	Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency	🟢	🟢	🟢	🟢
5.4.1	Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives	🟢	🟢	🟢	🟢
5.4.2	Expand Cyber Defense Collaboration with ICT Enablers	🟨	🟢	🟢	🟢

🟩 **5.1 – Codify the Concept of "Systemically Important Critical Infrastructure"**: *Nearing/partial implementation via executive action; further executive action required.* Prioritization among various critical infrastructure assets is imperative. NSM-22 tasked CISA with working with the other sector risk management agencies to identify systemically important entities (SIEs) within each critical infrastructure that have a disproportionate impact on U.S. national security, economic security, and public health and safety.[124] NSM-22, however, does not outline the benefits and burdens for companies identified as SIEs as explained in the Commission's initial recommendation on systemically important critical infrastructure. The administration and Congress must work together to detail the intelligence and information-sharing benefits and the minimum cybersecurity burdens of SIEs.

🟩 **5.1.1 – Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector**: *Nearing/partial implementation via executive action; further executive action required.* NSM-22 expands the responsibilities of the intelligence community, in coordination with the sector risk management agencies, to disseminate information to the private sector by producing intelligence reports "at the lowest possible classification level."[125] Additional congressional or executive branch action is necessary to examine foreign intelligence authorities, declassification procedures, and information-sharing consent processes.

🟩 **5.1.2 – Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities**: *Nearing/partial implementation via executive action; further legislative action required.* NSM-22 directs the director of national intelligence, in coordination with the Department of Homeland Security and sector risk management agencies, to identify and address the intelligence needs of critical infrastructure owners and operators.[126] To fully implement this recommendation, additional actions are required, including codifying legal protections to safeguard routinely shared information from public disclosure. The executive branch also needs to address the findings of an intelligence community audit released prior to NSM-22 detailing key limitations to sharing information with the private sector, including over-classification and inconsistent formats.[127]

🟩 **5.1.3 – Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities**: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by providing CISA with administrative subpoena authority.[128]

🟩 **5.2 – Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information**: *Nearing/partial implementation via appropriations; further legislative action required.* Last July, CISA announced plans to roll out a Joint Collaborative Environment (JCE).[129] CISA has begun work on establishing a JCE through the Cyber Analytics and Data Systems program that would aggregate and analyze data from various sources.[130] In the president's FY25 budget request, CISA requested $394.1 million for JCE, a much-needed investment following CISA's overall $34 million budget reduction in FY24.[131]

🟩 **5.2.1 – Expand and Standardize Voluntary Threat Detection Programs**: *Fully implemented via legislative action and appropriations.* The FY22 NDAA codified CyberSentry, a voluntary program through CISA that provides continuous monitoring and detection of cybersecurity threats on critical infrastructure networks.[132] This program meets the intent of this recommendation but only has 30 participating companies as of April 2024.[133]

🟩 **5.2.2 – Pass a National Cyber Incident Reporting Law**: *Fully implemented via legislative action and appropriations.* The passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as part of the FY22 consolidated appropriations bill, fully implemented this recommendation.[134] CISA is currently developing the final rule for CIRCIA implementation, having received industry feedback on its proposed rule.[135] Key suggestions from industry groups include harmonizing cyber reporting regulations, providing clear definitions for reporting requirements, and creating incentives for participation through timely threat information sharing.[136]

🟧 **5.2.3 – Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors**: *Progress limited; further legislative action required.* The Commission proposed an amendment to the Pen Register Trap and Trace Device Statute with the intent of allowing companies with the necessary resources and expertise to conduct more effective identifying activities on behalf of themselves or their customers. In 2021, the Commission shared with members of Congress a draft legislative text supporting this recommendation, but progress has been limited.

🟩 **5.3 – Strengthen an Integrated Cyber Center Within CISA and Promote the Integration of Federal Cyber Centers**: *Nearing/partial implementation via executive and legislative action; further executive action and appropriations required.* The efforts to "integrate federal cybersecurity centers" — strategic objective 1.3 of the National Cybersecurity Strategy — are ongoing. A February Government Accountability Office report recommended improving federal coordination, and there are signs of progress. In its strategic plan, CISA stated it would "exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents" with federal partners.[137] The second version of the National Cybersecurity Strategy Implementation Plan also notes that the ONCD completed an assessment of the capabilities of federal cybersecurity centers and will now focus on improving integration efforts.[138]

🟩 **5.4 – Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency**: *Fully implemented via legislative action and appropriations.* The FY21 NDAA fully implemented this recommendation.[139] Now known as CISA's Joint Cyber Defense Collaborative (JCDC), it has over 300 participating organizations, conducted over 1,000 pre-ransomware notifications during FY23, and has released more than 400 alerts and 1,116 operational cybersecurity products.[140] In her testimony before Congress on CISA's budget and the cyber threat from China, Director Jen Easterly noted that JCDC has developed 14 cyber defense plans.[141]

🟩 **5.4.1 – Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives**: *Fully implemented via legislative action and appropriations.* The FY22 NDAA implemented this recommendation,[142] and the Defense Department continues to demonstrate its commitment to improving public-private partnerships, emphasizing this in its latest cybersecurity strategy[143] and the first-ever National Defense Industrial Strategy.[144]

🟩 **5.4.2 – Expand Cyber Defense Collaboration With ICT Enablers**: *Fully implemented via legislative action.* The FY22 NDAA created voluntary and pilot programs that implemented this recommendation.[145]

Pillar 6: Preserve and Employ Military Instruments of Power

Preserve and Employ Military Instruments of Power

Rec. Number	Recommendation Title	2021	2022	2023	2024
6.1	Direct the DoD to Conduct a Force Structure Assessment of the Cyber Mission Force	🟩	🟩	🟩	🟩
6.1.1	Direct DoD to Create a Major Force Program Funding Category for U.S. Cyber Command	🟢	🟩	🟩	🟩
6.1.2	Expand Current Malware Inoculation Initiatives	🟧	🟨	🟨	🟨
6.1.3	Review Delegation of Authorities for Cyber Operations	🟩	🟩	🟩	🟩
6.1.4	Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces	🟧	🟧	🟧	🟨
6.1.5	Cooperate With Allies and Partners to Defend Forward	🟢	🟢	🟩	🟩
6.1.6	Require the DoD to Define Reporting Metrics	🟨	🟨	🟨	🟩
6.1.7	Assess the Establishment of a Military Cyber Reserve	🟩	🟢	🟢	🟢
6.1.8	Establish Title 10 Professors in Cyber Security and Information Operations	🟧	🟨	🟨	🟢
6.2	Conduct Cybersecurity Vulnerability Assessment Across the Nuclear Command, Control, and Communications and National Leadership Command Capability Systems & Continually Assess Weapon Systems' Cyber Vulnerabilities	🟩	🟩	🟩	🟩
6.2.1	Require DIB Participation in a Threat Intelligence Sharing Program	🟢	🟢	🟢	🟩
6.2.2	Require Threat Hunting on Defense Industrial Base Networks	🟢	🟢	🟢	🟢
6.2.3	Designate a Threat-Hunting Capability Across the DoD Information Network	🟧	🟩	🟩	🟩
6.2.4	Assess and Address the Risk to National Security Systems Posed by Quantum Computing	🟩	🟩	🟩	🟩

🟩 **6.1 – Direct DoD to Conduct a Force Structure Assessment of the Cyber Mission Force**: *Fully implemented via legislative action.* While the FY21 NDAA implemented this recommendation by mandating a force structure assessment, recent legislative actions reflect a continued concern about U.S. Cyber Command's operational readiness. Last year's NDAA contained provisions to enhance the capabilities, readiness, and resiliency of the Cyber Mission Force supporting this recommendation.[146] This year, both the House and Senate versions of the bill contain provisions requiring an independent study of how to improve cyber force generation in the U.S. military, including the possibility of creating a separate cyber service.[147]

🟩 **6.1.1 – Direct DoD to Create a Major Force Program Funding Category for U.S. Cyber Command**: *Fully implemented via legislative actions.* The FY21 and FY22 NDAAs implemented this recommendation providing U.S. Cyber Command with enhanced budgetary authority. The commissioners, however, remain concerned about U.S. Cyber Command's funding. While the president's FY25 budget request proposes a slight increase to $1.7 billion for U.S. Cyber Command,[148] the services still retain the vast majority of cyber-specific funding.[149] The Senate Armed Services Committee, meanwhile, plans to withhold funding for the Joint Cyber Warfighting Architecture until it receives a detailed plan from U.S. Cyber Command about its growth from 142 to 147 cyber mission force teams.[150]

🟨 **6.1.2 – Expand Current Malware Inoculation Initiatives**: *On track; further executive and legislative actions required.* The federal government used various interagency efforts to disclose information about malware[151] and indicators of compromise[152] to the public. U.S. Cyber Command, in particular, continues to share malware and other threat information with private partners through its Under Advisement program.[153] The Commission continues to believe that the statutory establishment of a Joint Collaborative Environment is necessary to further expand these efforts and meet the intent of this recommendation.

🟩 **6.1.3 – Review the Delegation of Authorities for Cyber Operations**: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by delegating cyber-related authorities to the commander of U.S. Cyber Command.[154]

🟨 **6.1.4 – Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces**: *On track; further executive action required.* There has been limited progress on this recommendation. The implementation of National Security Presidential Memorandum 13 over the past five years has significantly enhanced the process for planning and executing offensive cyber operations.[155] This improvement has had its most visible and acknowledged impact in efforts to protect U.S. elections in 2018, 2020, and 2022.[156] Additionally, U.S. Cyber Command has played an active role in assisting international allies and partners, including helping Ukraine defend its networks following the outbreak of war. As offensive cyber capabilities and activities continue to evolve, both independently and when integrated with kinetic operations, an update to the Standing Rules of Engagement and Standing Rules for the Use of Force for U.S. forces should reflect these changes.

🟩 **6.1.5 – Cooperate With Allies and Partners to Defend Forward**: *Fully implemented via executive action.* In the 2024 posture statement, newly confirmed U.S. Cyber Command Commander General Timothy Haugh reported that in 2023, U.S. Cyber Command had active hunt forward operations simultaneously across all geographic commands "for the first time."[157] Last year, U.S. Cyber Command conducted 22 hunt forward operations, a steady increase over prior years.[158]

Last year, U.S. Cyber Command conducted 22 hunt forward operations, a steady increase over prior years. U.S. Cyber Command Commander General Timothy Haugh (pictured above) reported that in 2023, U.S. Cyber Command had active hunt forward operations simultaneously across all geographic commands." (Photo by Chip Somodevilla/Getty Images)

🟩 **6.1.6 – Require DoD to Define Reporting Metrics**: *Fully implemented via legislative action.* The FY24 NDAA fully implemented this recommendation by mandating that the DoD establish performance metrics for the pilot program on sharing cyber capabilities with foreign partners.[159] Incorporating these metrics into the Cyber Mission Force's required[160] quarterly readiness assessments will further improve the ongoing evaluation of its cyber capabilities.

🟩 **6.1.7 – Assess the Establishment of a Military Cyber Reserve**: *Nearing/partial implementation via legislative action; further executive action required.* The FY24 NDAA authorized the secretary of the Army to conduct a pilot program on creating a civilian cybersecurity reserve.[161] This meets the intent of this recommendation. This progress is encouraging but does not yet fully implement this recommendation.

🟩 **6.1.8 – Establish Title 10 Professors in Cyber Security and Information Operations**: Nearing/*partial implementation via legislative action; further executive action required.* The FY24 NDAA[162] directed the Department of Defense to establish the Cyber Academic Engagement Office, which is responsible for fostering relationships with academic institutions, managing cyber-related educational programs, and overseeing the development of cyber skills within the U.S. military.[163] Although the establishment of Title 10 professors in cybersecurity and information operations remains unclear, these efforts enhance academic engagement and improve cyber education infrastructure, laying important groundwork.

🟩 **6.2 – Conduct a Cybersecurity Vulnerability Assessment Across the Nuclear Command, Control, and Communications and National Leadership Command Capability Systems & Continually Assess Weapon Systems' Cyber Vulnerabilities**: *Fully implemented via executive and legislative actions.* Previous legislation[164] and executive measures[165] mandated comprehensive reviews, evaluations, and the development of secure nuclear command, control, and communications (NC3) systems, fully implementing this recommendation. Additionally, last year, the FY24 included provisions establishing a Defense Department working group to inventory and mitigate risks, emphasizing continuous improvement and proactive measures for NC3 cybersecurity.

🟩 **6.2.1 – Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program**: *Fully Implemented via executive action.* In April 2024, a new rule went into effect, expanding the Defense Industrial Base (DIB) Cybersecurity Program to include all defense contractors with unclassified information systems handling covered defense information. This expansion grants an additional 68,000 contractors access to technical exchange meetings, a collaborative web platform, and threat information products and services through the Department of Defense Cyber Crime Center.[166] Additionally, the center and the Defense Counterintelligence and Security Agency announced a strategic partnership to launch a vulnerability disclosure program for the DIB.[167] The combination of the two efforts fully implemented this recommendation.

🟩 **6.2.2 – Require Threat Hunting on Defense Industrial Base Networks**: *Nearing/partial implementation via legislative action; further executive action required.* The FY21 NDAA[168] partially addressed this recommendation by mandating an assessment of the feasibility of implementing a defense industrial base cybersecurity threat-hunting program. In November 2023, the Defense Innovation Unit solicited comments on the Advanced Rapid Analysis of Cyber Hunt Network Infrastructure Data system,[169] requesting solutions for rapid threat hunting without requiring internet access or cloud resources, among other program requirements. This progress is encouraging but does not yet fully implement this recommendation.

🟩 **6.2.3 – Designate a Threat-Hunting Capability Across the DoD Information Network**: *Fully implemented via legislative action.* The FY22 NDAA implemented this recommendation by requiring threat hunting and discovery of malicious activity across the Defense Department's information network.[170]

🟩 **6.2.4 – Assess and Address the Risk to National Security Systems Posed by Quantum Computing**: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by requiring an assessment of the potential threats and risks posed by quantum computing.[171] Building on this, the FY24 NDAA includes a pilot program for quantum computing applications to address technical challenges and enhance capabilities.[172] Additionally, the House version of the FY25 NDAA includes a provision to create a Quantum Computing Center of Excellence within the Defense Department.[173]

CSC White Papers

In addition to its March 2020 report, the commission published a series of six white papers to address emerging issues and add greater detail to existing recommendations. The fifth white paper, not included below, was a transition book for the Biden administration, establishing priorities among existing recommendations but not offering new recommendations.

White Paper #1: Cybersecurity Lessons From the Pandemic

Cybersecurity Lessons From the Pandemic					
Rec. Number	Recommendation Title	2021	2022	2023	2024
PAN 1.1	Provide State, Local, Tribal, and Territorial Government and Small and Medium-sized Business IT Modernization Grants	🟨	🟢	🟩	🟩
PAN 1.2	Pass an Internet of Things Security Law	🟨	🟢	🟢	🟢
PAN 1.3	Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts	🟧	🟧	🟧	🟨
PAN 1.4	Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns	🟧	🟧	🟨	🟨
PAN 1.4.1	Establish the Social Media Data and Threat Analysis Center	🟢	🟨	🟢	🟢

🟩 **Pandemic 1.1 – Provide State, Local, Tribal, and Territorial Government and Small- and Medium-Sized Business Information Technology Modernization Grants**: *Fully implemented via legislative action.* The State and Local Cybersecurity Improvement Act, passed as part of the Infrastructure Investment and Jobs Act, implemented this recommendation.[174]

🟢 **Pandemic 1.2 – Pass an Internet of Things Security Law**: *Nearing/partial implementation via executive action; further legislation action required.* Last summer, the administration announced a cybersecurity certification and labeling program.[175] Earlier this year, the Federal Communications Commission approved the U.S. Cyber Trust Mark.[176] The details of the executive action are noted under recommendation 4.1 in this report. While the U.S. Cyber Trust Mark implements recommendation 4.1 and aligns with this recommendation, congressional action to codify an Internet of Things law is still necessary.

🟨 **Pandemic 1.3 – Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts**: *On track via appropriations; further executive action and appropriations required.* The Justice Department's Office of Justice Programs announced a new funding opportunity in June to help state, local, territorial, and tribal law enforcement better handle financial, technological, and internet crimes through training and support programs. This funding provides eligible nonprofit and education institutions essential resources for developing and updating training materials and supporting joint initiatives between law enforcement, prosecutors, and judges.[177]

🟨 **Pandemic 1.4 – Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns**: *On track via appropriations; further appropriations required*. The Department of State's Global Engagement Center (GEC) provides grants to nonprofit institutions to research Russian propaganda and other disinformation-related topics.[178] The National Science Foundation (NSF) has also previously provided grant funding for disinformation research.[179] As originally envisioned by the Commission, implementing this recommendation would require Congress to authorize and appropriate funds for a grant program within the Department of Justice. However, Congress could achieve the intent of this recommendation through GEC, NSF, or other grant programs, provided they are sufficiently funded.

🟢 **Pandemic 1.4.1 – Establish the Social Media Data and Threat Analysis Center**: *Nearing/partial implementation via legislative action; further executive action required.* The FY23 NDAA directed the director of national intelligence (DNI) to submit "a plan to operationalize" the Social Media and Threat Analysis Center.[180] The DNI has not yet submitted the plan to Congress.

White Paper #2: National Cyber Director

National Cyber Director					
Rec. Number	Recommendation Title	2021	2022	2023	2024
NCD 1	Establish a National Cyber Director Position	🟩	🟩	🟩	🟩

🟩 **Establish a National Cyber Director**: *Fully implemented via legislative and executive action and appropriations.* The FY21 NDAA created the ONCD.[181] Since then, the office staff has grown, and the FY24 omnibus spending bill authorized $21.7 million for the ONCD.[182] For FY25, the ONCD proposed a budget of $19 million, a slight decrease from previous years due to prior investments in secure facilities in FY23.[183] Over the past year, the ONCD has implemented nearly 50 percent of the 69 initial initiatives outlined in the original National Cybersecurity Strategy Implementation Plan.[184] According to the ONCD and the OMB joint memorandum from July 2024, the two agencies will jointly review cybersecurity priorities and investments for the federal government.[185]

White Paper #3: Growing a Stronger Federal Cyber Workforce

Growing a Stronger Federal Cyber Workforce					
Rec. Number	Recommendation Title	2021	2022	2023	2024
WF 1	Establish Leadership and Coordination Structures	🟧	🟨	🟢	🟩
WF 2	Properly Identify and Utilize Cyber-Specific Occupational Classifications	🟧	🟨	🟨	🟢
WF 3	Develop Apprenticeships	🟨	🟢	🟢	🟩
WF 4	Improve Cybersecurity for K-12 Schools	🟨	🟢	🟢	🟢
WF 5	Provide Work-Based Learning via Volunteer Clinics	🟧	🟧	🟢	🟩
WF 6	Improve Pay Flexibility and Hiring Authority	🟧	🟨	🟨	🟢
WF 7	Incentivize Cyber Workforce Research	🟨	🟩	🟩	🟩
WF 8	Mitigate Retention Barriers and Invest in Diversity, Equity, and Inclusion in Recruiting	🟧	🟨	🟢	🟢

🟩 **Workforce 1 – Establish Leadership and Coordination Structures**: *Fully implemented via executive action.* In June 2024, the ONCD released a progress report on implementing the National Cybersecurity Workforce and Education Strategy. Since creating the National Cyber Workforce Coordination Group in early 2023, the ONCD has established the Working Group on Cyber Workforce and Education and the Working Group on Cyber Skills and Awareness, fully implementing this recommendation. According to the progress report, "more than 35 federal departments and agencies [...] have begun implementing the objectives" in the strategy and are "willing to make additional voluntary commitments" in the next year to engage with industry partners to improve the national cyber workforce.[186]

🟩 **Workforce 2 – Properly Identify and Utilize Cyber-Specific Occupational Classifications**: *Nearing/partial implementation via executive action; further executive action required.* At a White House convening on the national cybersecurity workforce in April 2024, National Cyber Director Coker announced plans to transition nearly 100,000 federal jobs to skill-based hiring by the summer of 2025 instead of relying on four-year degree requirements.[187] Assistant National Cyber Director Seeyew Mo testified before the House Committee on Homeland Security that removing such barriers is "the only way we can defend the digital foundation of our modern way of life."[188]

🟩 **Workforce 3 – Develop Apprenticeships**: *Fully implemented via executive and legislative actions.* In March 2024, President Biden issued Executive Order 14119 "Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums."[189] A month prior, the Department of Labor (DoL) allocated $95 million for federal and $100 million for state apprenticeship programs.[190] Last year, DoL awarded nearly $108 million for these programs, according to the National Cyber Workforce and Education Strategy Implementation progress report published in June 2024.[191]

🟩 **Workforce 4 – Improve Cybersecurity for K-12 Schools**: *Nearing/partial implementation via executive and legislative actions; further appropriations required.* Last year, the Department of Education released guidance documents, including the "K-12 Digital Infrastructure Brief: Defensible and Resilient," to help bolster the sector's cybersecurity posture.[192] In March 2024, the Department of Education and CISA announced the establishment of a Government Coordinating Council dedicated to enhancing collaboration between federal, state, and local governments for K-12 cybersecurity,[193] aligned with the call to action as issued in NSM-22.[194]

🟩 **Workforce 5 – Provide Work-Based Learning via Volunteer Clinics**: *Fully implemented via executive and legislative actions.* In 2023, the NSA established Cyber Clinics in four states to support communities and small governments with cyber risk assessment and planning assistance to which they "would otherwise not have access." According to the latest cyber workforce implementation plan, this model has attracted "more than $25 million in private sector investment that has enabled the opening of clinics at 45 more institutions."[195] Private sector companies, such as Google, are pursuing and funding similar efforts.[196]

🟩 **Workforce 6 – Improve Pay Flexibility and Hiring Authorities**: *Nearing/partial implementation via executive action; further executive and legislative actions required.* The Office of Personnel Management (OPM) and the ONCD proposed legislative changes to cyber workforce classification and pay systems commonly used throughout the federal government. The proposal includes higher special pay rates and more streamlined hiring procedures.[197] In October 2023, OPM published an action plan for "Strengthening Officer Recruitment, Hiring, Promotion, and Retention," including cybersecurity personnel.[198] In a similar trend, OPM published a memorandum in February 2024 urging federal agencies to provide incentive pay and leave flexibilities to recruit and retain artificial intelligence-related talent.[199]

🟩 **Workforce 7 – Incentivize Cyber Workforce Research**: *Fully implemented via legislative action and appropriations.* The passage of the CHIPS and Science Act fully implemented this recommendation.[200]

🟩 **Workforce 8 – Mitigate Retention Barriers and Invest in Diversity in Recruiting**: *Nearing/partial implementation via executive and legislative actions; further executive and legislative actions and appropriations required.* There have been various efforts underway to create an inclusive cybersecurity workforce in the federal government following the issuance of the June 2021 Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce.[201] Following National Cyber Director Coker's update on eliminating four-year degree requirements from certain federal jobs,[202] the administration committed to building a diverse and skilled pipeline of cybersecurity talent in advanced manufacturing through similar efforts.[203] The federal government plans to accomplish this by the summer of 2025.[204] In July 2024, the Federal Cyber Workforce Training Act passed the Senate Homeland Security and Governmental Affairs Committee. Co-sponsored by Sens. Mike Rounds (R-SD) and Jon Ossoff (D-GA), the bill proposes creating a Federal Cyber Workforce Development Institute to provide skill-based training to early and mid-career federal cybersecurity employees.[205] The bill is scheduled for a full Senate vote in September when Congress reconvenes.[206] Additionally, CISA has partnered with industry to launch a 15-month-long initiative known as the Neurodiverse Federal Workforce. This initiative could help address high unemployment rates among the neurodiverse population[207] and help inform policies to "increase opportunities for neurodiverse individuals who are on the autism spectrum."[208] In April 2024, the National Institute of Standards and Technology awarded $3.6 million to 18 organizations across 15 states focused on addressing the national cybersecurity workforce shortage through education and training development programs.[209]

White Paper #4: Building a Trusted ICT Supply Chain

Building a Trusted ICT Supply Chain					
Rec. Number	Recommendation Title	2021	2022	2023	2024
SC 1	Develop and Implement an ICT Industrial Base Strategy	🟢	🟩	🟩	🟩
SC 2	Identify Key ICTs and Materials	🟢	🟩	🟩	🟩
SC 3	Conduct a Study on the Viability of and Designate Critical Technology Clusters	🟢	🟩	🟩	🟩
SC 3.1	Provide Research and Development Funding for Critical Technologies	🟨	🟩	🟩	🟩
SC 3.2	Incentivize the Movement of Critical Chip and Technology Manufacturing out of China	🟨	🟩	🟩	🟩
SC 3.3	Conduct a Study on a National Security Investment Corporation	🟨	🟨	🟧	🟨
SC 4	Designate Lead Agency for ICT Supply Chain Risk Management	🟢	🟩	🟩	🟩
SC 4.1	Establish a National Supply Chain Intelligence Center	🟨	🟧	🟨	🟢
SC 4.2	Fund Critical Technology Security Centers	🟨	🟢	🟢	🟢
SC 5	Incentivize Open and Interoperable Standards and Release More Mid-Band Spectrum	🟧	🟢	🟢	🟩
SC 5.1	Develop a Digital Risk Impact Assessment for International Partners for Telecommunications Infrastructure Projects	🟨	🟨	🟨	🟢
SC 5.2	Ensure That the EXIM, DFC, and USTDA Can Compete with Chinese State-owned and State-backed Enterprises	🟨	🟢	🟢	🟢
SC 5.3	Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects	🟨	🟨	🟨	🟨

🟩 **Supply Chain 1 – Develop and Implement an ICT Industrial Base Strategy**: *Fully implemented via executive action.* The February 2021 supply chain executive order directing federal agencies to assess strategic risks to protect the information communications technology (ICT) supply chain fully implemented this recommendation.[210] This year, efforts continue as CISA is renewing its ICT Supply Chain Risk Management Task Force.[211]

🟩 **Supply Chain 2 – Identify Key ICTs and Materials**: *Fully implemented via executive and legislative actions and appropriations.* The February 2022 "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry" fully implemented this recommendation.[212]

🟩 **Supply Chain 3 – Conduct a Study on the Viability of Critical Technology Clusters and Designate Them**: *Fully implemented via legislative action and appropriations.* The passage of the CHIPS and Science Act, which established a regional technology and innovation hubs program at the Department of Commerce, fully implemented this recommendation.[213] In October 2023, the administration announced 31 tech hubs across the country[214] and in July 2024 selected 12 recipients to receive a total of $504 million in grant funding to advance work in industries such as semiconductors, climate and energy, biotechnology, and quantum computing.[215]

🟩 **Supply Chain 3.1 – Provide Research and Development Funding for Critical Technologies**: *Fully implemented via legislative action and appropriations.* The CHIPS and Science Act implemented this recommendation and spurred additional investments in research and development for critical technologies. For instance, in February 2024, the administration announced plans to invest $5 billion in the National Semiconductor Technology Center, a "public-private consortium" focused on research and development and workforce initiatives.[216]

🟩 **Supply Chain 3.2 – Incentivize the Movement of Critical Chip and Technology Manufacturing Out of China**: *Fully implemented via legislative action and appropriations.* The CHIPS and Science Act provided more than $50 billion to boost the U.S. domestic chip industry, leading to nearly $450 billion in private investments. According to the Semiconductor Industry Association, these investments are expected to create over 56,000 jobs across the country.[217]

🟨 **Supply Chain 3.3 – Conduct a Study on a National Security Investment Corporation**: *On track; further legislative action required.* The Commission drafted legislation mandating a study assessing the possible impacts of establishing a National Security Investment Corporation. While Congress has not yet taken up this legislation, other efforts within the federal government align with this recommendation. Established in December 2022, the Defense Department's Office of Strategic Capital fosters private investment in critical technology sectors. In March 2024, the office released its first Investment Strategy, identifying priority areas such as space, artificial intelligence, cybersecurity, and quantum computing, with a requested budget of $144 million for FY25.[218]

🟩 **Supply Chain 4 – Designate a Lead Agency for the ICT Supply Chain**: *Fully implemented via executive and legislative actions; further appropriations required.* The FY21 NDAA designated the Department of Homeland Security as the sector risk management agency for the information technology sector, fully implementing this recommendation.[219] NSM-22 also reaffirms this designation.

🟩 **Supply Chain 4.1 – Establish a National Supply Chain Intelligence Center**: *Nearing/partial implementation via legislative action; further executive and legislative actions required.* The FY20 NDAA established a Supply Chain and Counterintelligence Risk Management Task Force to share sensitive information with the federal acquisition community. This effort is led by the National Counterintelligence and Security Center (NCSC). The NCSC established the Supply Chain and Cyber Directorate to enhance the nation's supply chain and cybersecurity, leveraging counterintelligence and security expertise to inform, guide, and coordinate integrated risk decisions and responses with strategic partners. Subsequently, in June 2024, the Supply Chain Optimization and Intelligence Network's two-year NIST pilot program, authorized by the CHIPS and Science Act, completed its first year. This network of 51 manufacturing extension partnership centers bolsters domestic manufacturing resilience by mapping capabilities and sharing supply chain intelligence.[220] While both of these efforts are aligned with the recommendation's intent, Congress should establish a permanent center for full implementation.

🟩 **Supply Chain 4.2 – Fund Critical Technology Security Centers**: *Nearing/partial implementation via legislative action; further legislative action required.* The Infrastructure Investment and Jobs Act partially implemented this recommendation.[221] While there has been congressional interest in creating critical technology security centers,[222] legislation has not yet passed.

🟩 **Supply Chain 5 – Incentivize Open and Interoperable Standards and Release More Mid-band Spectrum**: *Fully implemented via executive and legislative actions and appropriations.* In September 2023, the Department of Defense published a feasibility assessment report on repurposing mid-band spectrum for commercial use and accompanying recommendations, fully implementing this recommendation.[223] Two months later, the National Telecommunications and Information Administration published its National Spectrum Strategy, providing examples of ongoing efforts to release more mid-band spectrum.[224] The administration also announced a $420 million funding opportunity in May 2024 to advance open network adoption by developing open radio units, crucial for building secure and innovative wireless equipment.[225]

🟩 **Supply Chain 5.1 – Develop a Digital Risk Impact Assessment for International Partners for Telecom Infrastructure Projects**: *Nearing/partial implementation via executive action; further executive action required.* Promoting trusted and secure telecommunications infrastructure has been a major focus of the State Department's Bureau of Cyberspace and Digital Policy. During his trip to Australia and Fiji in January 2024, CDP Ambassador-at-Large Nathaniel Fick met with Pacific Island leaders to promote the use of trusted vendors for undersea cables.[226] With $50 million for the Digital Connectivity and Cybersecurity Partnership initiative, CDP has been working with allies and partners like Japan and Australia to counter Chinese influence in the Pacific region.[227]

🟩 **Supply Chain 5.2 – Ensure That the Export-Import Bank, U.S. International Development Finance Corporation, and U.S. Trade Development Agency Can Compete With Chinese State-Owned and State-Backed Enterprises**: *Nearing/partial implementation via legislative action; further executive and legislative actions required.* The CHIPS and Science Act partially implemented this recommendation.[228] However, the Export-Import Bank (EXIM) and International Development Finance Corporation (DFC) remain unable to offer loans that rival the more attractive Chinese offers in terms of rates, terms, or conditions to borrowers. Though some individual cases have been successful,[229] this process does not produce systemic improvements. This limitation stems from EXIM/DFC lending requirements, which must comply with Office of Management and Budget circulars in accordance with the 1991 Federal Credit Reform Act.[230] As a result, EXIM/DFC cannot offer concessional loans, or loans below comparable Treasury notes. But by offering rates lower than market levels, EXIM/DFC would effectively provide borrowers subsidized financing for projects. Similar rules govern loan tenure, or the repayment period. The U.S. Trade Development Agency (USTDA) operates under a different model, primarily offering grants for bankable feasibility studies and reverse trade missions.[231] While this approach is valuable, it addresses only part of the competitive landscape. The efficacy of USTDA's efforts is contingent upon subsequent backing from project developers or financial institutions willing to pick up the project post-USTDA involvement. Without their engagement, the initial groundwork may prove futile.

🟨 **Supply Chain 5.3 – Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects**: *On track via executive action; further executive and legislative actions required.* While Congress and the Biden administration remain focused on limiting the ability of Chinese state-controlled companies to do business in the United States,[232] the administration needs to create a comprehensive list of prohibited contractors to fully implement this recommendation.

White Paper #6: Countering Disinformation in the United States

Countering Disinformation in the United States					
Rec. Number	**Recommendation Title**	**2021**	**2022**	**2023**	**2024**
CD 1	Establish a Civic Education Task Force, Enable Greater Access to Civic Education Resources, and Raise Public Awareness	N/A	🟨	🟩	🟩
CD 2	Ensure Material Support for Nongovernmental Disinformation Researchers	N/A	🟧	🟩	🟩
CD 3	Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public	N/A	🟧	🟨	🟨
CD 4	Create a Capability within the Department of Homeland Security to Actively Monitor Foreign Disinformation	N/A	🟧	🟧	🟧
CD 5	Create a Grants Program to Equip State and Local Governments	N/A	🟧	🟩	🟩
CD 6	Reform the Foreign Agents Registration Act and Introduce New Federal Communications Commission Regulations	N/A	🟧	🟨	🟨
CD 7	Publish and Enforce Transparency Guidelines for Social Media Platforms	N/A	🟧	🟧	🟧

🟩 **Countering Disinformation 1 – Establish a Civic Education Task Force, Enable Greater Access to Civic Education Resources, and Raise Public Awareness**: *Nearing/partial implementation via legislative action and appropriations; further executive action required.* Over the past two years, Congress has appropriated consistent funding of $23 million to the Department of Education for civic education,[233] and the president's FY25 budget request proposes the same.[234] According to iCivics, a nonprofit organization that promotes civics education, the funding provided seven additional grant opportunities in 2023 for programs training educators and improving civics education curriculum.[235] Despite these advancements, ensuring consistent access and impact across all states remains a challenge.

🟩 **Countering Disinformation 2 – Ensure Material Support for Nongovernmental Disinformation Researchers**: *Nearing/partial implementation via appropriations; further legislative action and appropriations required.* The National Science Foundation (NSF) continues to provide grants for disinformation. However, the House Judiciary Committee criticized NSF for funding projects the committee alleged were potential tools for censorship.[236] Congress struggles to reach a consensus on the direction and importance of disinformation research. Clear legislative guidance is crucial to align public and governmental expectations and ensure consistent funding for anti-disinformation research.

🟨 **Countering Disinformation 3 – Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public**: *On track via executive action and appropriations; further appropriations required.* In June 2024, the State Department released a Framework to Counter Foreign State Information Manipulation, which seeks to establish "a coordinated international response" to this threat.[237] The State Department maintained grant opportunities in FY24 and requested $2 million for the Global Engagement Center in FY25 to protect the American public from malign foreign influence campaigns.[238] Amid Republican criticism, Secretary of State Antony Blinken advocated for the center's funding, testifying to Congress that the center plays a critical role in "countering the threat of information manipulation by China, by Russia, and others."[239]

🟧 **Countering Disinformation 4 – Create a Capability Within DHS to Actively Monitor Foreign Disinformation**: *Progress limited via legislative action; further executive action required.* Progress on efforts aligned with this recommendation has stalled since the disbandment of the Disinformation Governance Board in 2022.[240] Last year, several House Republican lawmakers argued that the Biden administration "strong-armed Big Tech companies" to suppress conservative viewpoints and censor content that did not align with their political agenda.[241] This led to the U.S. Supreme Court case *Murthy v. Missouri*. In June 2024, the Supreme Court ruled that the Biden administration is not censoring content on social media platforms and is allowed to engage with these companies. Following the ruling, CISA Director Jen Easterly reiterated that "CISA does not and has never censored speech."[242]

🟩 **Countering Disinformation 5 – Create a Grant Program to Equip State and Local Governments**: *Nearing/partial implementation via appropriations; further appropriations required.* The Department of Homeland Security continues to provide grant funding to counter disinformation through the Homeland Security Grant Program.[243] Additionally, in May 2024, CISA and the Election Assistance Commission published guidance to aid state, local, tribal, and territorial governments in developing public communications plans to "mitigate risks to election infrastructure."[244]

🟨 **Countering Disinformation 6 – Reform the Foreign Agents Registration Act (FARA) and Introduce New Federal Communications Commission Regulations**: *On track via legislative action; further legislative action required.* There continues to be congressional interest in the Preventing Adversary Influence, Disinformation, and Obscured Foreign Financing Act, which aims to remove Foreign Agents Registration Act exemptions for media entities,[245] but ultimately, Congress has failed to pass this bill. Last year, it was included in the Senate version of the FY24 NDAA but removed from the final bill.[246] This year, House members pushed to include a similar provision in the FY25 NDAA, but it was not included in their final version.[247]

🟧 **Countering Disinformation 7 – Publish and Enforce Transparency Guidelines for Social Media Platforms**: *Progress limited; further legislative action required.* During the markup of the FY25 homeland security appropriations bill, the Republican committee members rejected amendments to label "constitutionally protected speech" as mis/disinformation or "malinformation."[248] While Congress passed a law forcing TikTok's parent company to sell the platform or face a U.S. ban, this legislation focused on the unique national security risk posed by Chinese-ownership of this platform rather than on transparency guidelines for social media content more generally.[249]

Conclusion

Over the past four years, both the Biden-Harris administration and lawmakers have spurred substantial advances in cybersecurity, implementing many of the U.S. Cyberspace Solarium Commission's recommendations. Looking ahead, CSC 2.0 will continue to conduct research to advance the Commission's policy recommendations. The ongoing efforts assessed in this report are essential to maintaining and enhancing the nation's cybersecurity posture. The collaboration between government and private sector partners will continue to be pivotal in addressing emerging threats and ensuring the resilience and security of critical infrastructure for the incoming administration. The foundation laid by the current administration will be instrumental in guiding the future cybersecurity policy landscape to fortify the U.S. national security and economic prosperity.

Endnotes

1. Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center, “Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double,” February 2024, page 1. (https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf)

2. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4091. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=705)

3. The White House, “Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy,” March 2, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy)

4. The White House, “National Cybersecurity Strategy Implementation Plan,” May 4, 2024. (https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf)

5. Executive Office of the President, Office of the National Cyber Director, “2024 Report on the Cybersecurity Posture of the United States,” May 2024, page 14. (https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf)

6. The White House, Press Release, “Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan,” May 7, 2024. (https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2)

7. The White House, “National Cybersecurity Strategy,” March 1, 2023, page 14. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

8. U.S. Department of State, Press Release, “Release of United States’ International Cyberspace and Digital Policy Strategy,” May 6, 2024. (https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy)

9. Loper Bright Enterprises v. Raimondo, No. 22-451, 603 (D.D.C. 2024) (https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf)

10. U.S. Government Accountability Office, “Fiscal Year 2025 Budget Request,” May 8, 2024, pages 2-5. (https://www.appropriations.senate.gov/imo/media/doc/download_testimony46.pdf)

11. U.S. Senate Committee on Appropriations, “Bill Summary: Legislative Branch Fiscal Year 2024 Appropriations Bill,” March 21, 2024, page 3. (https://www.appropriations.senate.gov/imo/media/doc/fy24_leg_branch_bill_summary.pdf); Library of Congress, “Library of Congress Fiscal 2025 Budget Justification,” page 125. (https://loc.gov/static/portals/about/reports-and-budgets/documents/budgets/fy2025.pdf)

12. United States Senate, “Roll Call Vote 118th Congress - 1st Session,” accessed August 12, 2024. (https://www.senate.gov/legislative/LIS/roll_call_votes/vote1181/vote_118_1_00337.htm)

13. The White House, “About the Director,” accessed August 12, 2024. (https://www.whitehouse.gov/oncd/about-the-director)

14. Martin Matishak, “Latest government funding bill makes modest cut to CISA,” *The Record*, March 21, 2024. (https://therecord.media/government-funding-bill-makes-modest-cisa-cuts)

15. U.S. Cybersecurity and Infrastructure Security Agency Director Jen Easterly, “Opening Statement,” *Testimony before the House Committee on Appropriations, Subcommittee on Homeland Security on the Fiscal Year 2025 Budget for the Cybersecurity and Infrastructure Security Agency*, April 30, 2024. (https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly-0); Cate Burgan, “Easterly: China Threat Drives FY2025 Budget Boost Request,” *MeriTalk*, May 1, 2024. (https://www.meritalk.com/articles/easterly-china-threat-drives-fy2025-budget-boost-request); Tim Starks, “Easterly appeals to Congress on CISA funding, citing Chinese threats to critical infrastructure,” *CyberScoop*, April 30, 2024. (https://cyberscoop.com/jen-easterly-cisa-funding-congress-critical-infrastructure-china)

16. The White House, “National Security Memorandum on Critical Infrastructure Security and Resilience,” April 30, 2024. (https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience)

17. Consolidated Appropriations Act, 2022, Pub. L. 117-103, 136 Stat. 1034. (https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf)

18. “CTIIC Products,” *Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center*, accessed August 12, 2024. (https://www.odni.gov/index.php/ctiic-what-we-do/ctiic-products); The White House, “National Security Memorandum on Critical Infrastructure Security and Resilience,” April 30, 2024. (https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience)

19. U.S. Federal Bureau of Investigation Directory Christopher Wray, “A Review of the President’s Fiscal Year 2025 Budget Request for the Federal Bureau of Investigation,” *Statement before the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies*, June 4, 2024. (https://www.fbi.gov/news/testimony/a-review-of-the-president-s-fiscal-year-2025-budget-request-for-the-federal-bureau-of-investigation)

20. U.S. Department of Justice, Federal Bureau of Investigation, “FY 2025 Budget Request At A Glance,” accessed August 12, 2024, pages 1-2. (https://www.justice.gov/d9/2024-03/bs_section_ii_chapter_-_fbi_3-4-24_final_1.pdf)

21. AJ Vicens, “The FBI is adding more cyber-focused agents to U.S. embassies,” *CyberScoop*, January 3, 2024. (https://cyberscoop.com/the-fbi-is-adding-more-cyber-focused-agents-to-u-s-embassies); RADM (Ret.) Mark Montgomery and Jiwon Ma, “Targeting FBI Budget Makes Us More Vulnerable on Cyber,” *Cipher Brief*, December 1, 2023. (https://www.thecipherbrief.com/column/cyber-advisor/targeting-fbi-budget-makes-us-more-vulnerable-on-cyber)

22. U.S. Office of Personnel Management, Press Release, “Release: New OPM Workforce of the Future Playbook Prioritizes a Skilled, Inclusive, and Agile and Engaged Federal Workforce,” February 23, 2024. (https://www.opm.gov/news/releases/2024/02/release-new-opm-workforce-of-the-future-playbook-prioritizes-a-skilled-inclusive-and-agile-and-engaged-federal-workforce); U.S. Office of Personnel Management, “Playbook for Implementing Strategies to Enable a Federal Workforce that is Inclusive, Agile and Engaged, with the Right Skills to Enable Mission Delivery,” February 2024. (https://www.opm.gov/workforce-of-the-future/wof-playbook.pdf)

23. U.S. National Institute for Standard and Technology, “NIST Awards $3.6 Million for Community-Based Cybersecurity Workforce Development,” April 3, 2024. (https://www.nist.gov/news-events/news/2024/04/nist-awards-36-million-community-based-cybersecurity-workforce-development)

24. U.S. Department of Labor, Press Release, “US Department of Labor Awards More Than $39m in Grants to Expand, Diversify State Registered Apprenticeship Programs,” July 10, 2024. (https://www.dol.gov/newsroom/releases/eta/eta20240710)

25. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, Press Release, “CISA Awards $3M in Funding for Cyber Education and Training of Next-Gen Cyber Leaders,” November 3, 2023. (https://www.cisa.gov/news-events/news/cisa-awards-3m-funding-cyber-education-and-training-next-gen-cyber-leaders)

26. U.S. Department of Homeland Security, “Cybersecurity and Infrastructure Security Agency Budget Overview Fiscal Year 2025 Congressional Justification,” accessed August 12, 2024, page 108. (https://www.dhs.gov/sites/default/files/2024-04/2024_0318_cybersecurity_and_infrastructure_security_agency.pdf)

27. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3898. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf#page=1504)

28. “PN2223 – Nathaniel Fick – Department of State,” *Congress.gov*, September 15, 2022. (https://www.congress.gov/nomination/117th-congress/2223?s=1&r=95)

29. U.S. Department of State, Press Release, “Release of United States’ International Cyberspace and Digital Policy Strategy,” May 6, 2024. (https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy)

30. U.S. Government Accountability Office, “Cyber Diplomacy: State’s Efforts Aim to Support U.S. Interests and Elevate Priorities,” January 11, 2024, page 22. (https://www.gao.gov/assets/d24105563.pdf)

31. U.S. Department of State, “Discussions on Deterring Malicious Cyber Activity and the UN Framework of Responsible State Behavior in Cyberspace,” June 17, 2024. (https://www.state.gov/discussions-on-deterring-malicious-cyber-activity-and-the-un-framework)

32. European Commission, “EU-US Joint Statement on CyberSafe Products Action Plan,” January 31, 2024. (https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan)

33. The White House, “Joint Statement Endorsing Principles for 6G: Secure, Open, and Resilient by Design,” February 26, 2024. (https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/26/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design)

34. The White House, “U.S.-EU Joint Statement of the Trade and Technology Council,” April 5, 2024. (https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3); European Commission, “EU-US Trade and Technology Council (2021-2024),” May 3, 2024. (https://digital-strategy.ec.europa.eu/en/factpages/eu-us-trade-and-technology-council-2021-2024); Executive Office of the President, Office of the United States Trade Representative, “U.S.-E.U. Trade and Technology Council (TTC),” accessed August 12, 2024. (https://ustr.gov/useuttc)

35. U.S. Department of Energy, “DOE Leads Effort to Improve the Cybersecurity of Energy Supply Chains,” June 18, 2024. (https://www.energy.gov/articles/doe-leads-effort-improve-cybersecurity-energy-supply-chains)

36. U.S. Department of Commerce, National Telecommunications and Information Administration, “Rwanda Recap: U.S. Support for Multistakeholder Internet Governance at ICANN80,” July 1, 2024. (https://www.ntia.gov/blog/2024/rwanda-recap-us-support-multistakeholder-internet-governance-icann80)

37. U.S. Department of State, Bureau of Cyberspace and Digital Policy, “United States’ International Cyberspace and Digital Policy Strategy,” May 6, 2024, pages 19-26. (https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy); “U.S. Department of State, “Co-Chairs’ Statement on the Fourth ASEAN-U.S. Cyber Policy Dialogue,” November 7, 2023, pages 19 and 26. (https://www.state.gov/co-chairs-statement-on-the-fourth-asean-u-s-cyber-policy-dialogue)

38. U.S. Department of State, “United States International Cyberspace & Digital Policy Strategy Towards an Innovative, Secure, and Rights-Respecting Digital Future,” May 6, 2024. (https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy)

39. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 990. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=856)

40. Further Consolidated Appropriations Act, 2024, H.R. 2882, 118th Congress (2024). (https://www.congress.gov/bill/118th-congress/house-bill/2882/text#H082E0B6446D24329841C455F099669A7); Eric Geller, "America's cyber ambassador on how to spend $50 million in foreign aid," *The Record*, April 22, 2024. (https://therecord.media/cyber-foreign-aid-nathaniel-fick-state-department)

41. Jacob Livesay, "House appropriators advance State Dept. bill with cyber capacity-building funds," *Inside Cybersecurity*, June 18, 2024. (https://insidecybersecurity.com/daily-news/house-appropriators-advance-state-dept-bill-cyber-capacity-building-funds)

42. AJ Vicens, "The FBI is adding more cyber-focused agents to U.S. embassies," *CyberScoop*, January 3, 2024. (https://cyberscoop.com/the-fbi-is-adding-more-cyber-focused-agents-to-u-s-embassies)

43. U.S. Federal Bureau of Investigation Cyber Division Assistant Director Bryan A. Vorndran, "Oversight of the FBI Cyber Division," Statement before the House Judiciary Committee, March 29, 2022. (https://www.fbi.gov/news/testimony/oversight-of-the-fbi-cyber-division-032922); RADM (Ret.) Mark Montgomery and Jiwon Ma, "Targeting FBI Budget Makes Us More Vulnerable on Cyber," *Cipher Brief*, December 1, 2023. (https://www.thecipherbrief.com/column/cyber-advisor/targeting-fbi-budget-makes-us-more-vulnerable-on-cyber)

44. House Appropriations Committee Democrats, Press Release, "Republicans Defund Law Enforcement, Hurt Communities, Advantage Tax Cheats in 2024 Commerce, Justice, Science, and Related Agencies Funding Bill," July 13, 2023. (https://democrats-appropriations.house.gov/news/press-releases/republicans-defund-law-enforcement-hurt-communities-advantage-tax-cheats-in-2024)

45. Executive Order 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," September 12, 2018. (https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election)

46. The White House, "Notice on the Continuation of the National Emergency With Respect to Foreign Interference In or Undermining Public Confidence in United States Elections," September 7, 2022. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/07/notice-on-the-continuation-of-the-national-emergency-with-respect-to-foreign-interference-in-or-undermining-public-confidence-in-united-states-elections-2); The White House, Press Release, "Notice on the Continuation of the National Emergency with Respect to Foreign Interference in or Undermining Public Confidence in United States Elections," September 7, 2023. (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/09/07/press-release-notice-on-the-continuation-of-the-national-emergency-with-respect-to-foreign-interference-in-or-undermining-public-confidence-in-united-states-elections)

47. U.S. Department of the Treasury, Office of Foreign Assets Control, "Cyber-related Designation Removal; Russia-related Designation Removal; Issuance of Venezuela General License 40C," July 8, 2024. (https://ofac.treasury.gov/recent-actions/20240708); U.S. Department of the Treasury, Office of Foreign Assets Control, Press Release, "Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure," February 2, 2024. (https://home.treasury.gov/news/press-releases/jy2072); U.S. Department of the Treasury, Office of Foreign Assets Control, Press Release, "Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies," April 23, 2024. (https://home.treasury.gov/news/press-releases/jy2292); U.S. Department of the Treasury, Office of Foreign Assets Control, Press Release, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," February 2, 2024. (https://home.treasury.gov/news/press-releases/jy2072)

48. U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Charges Four Iranian Nationals for Multi-Year Cyber Campaign Targeting U.S. Companies," April 23, 2024. (https://www.justice.gov/opa/pr/justice-department-charges-four-iranian-nationals-multi-year-cyber-campaign-targeting-us); @RFJ_USA, *X*, April 23, 2024. (https://x.com/RFJ_USA/status/1782824365127500272)

49. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," May 24, 2023. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a)

50. U.S. National Security Agency, Press Release, "NSA and Partners Spotlight People's Republic of China Targeting of U.S. Critical Infrastructure," February 7, 2024. (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669141/nsa-and-partners-spotlight-peoples-republic-of-china-targeting-of-us-critical-i)

51. Mike Cherney, "U.S., Allies Issue Rare Warning on Chinese Hacking Group," *The Wall Street Journal*, July 9, 2024. (https://www.wsj.com/politics/national-security/u-s-allies-issue-rare-warning-on-chinese-hacking-group-9eebb0ce?mod=djemCybersecruityPro&tpl=cs)

52. Executive Office of the President, Office of the National Cyber Director, "2024 Report on the Cybersecurity Posture of the United States," May 2024, page 13. (https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf)

53. U.S. Government Accountability Office, "Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities," January 11, 2024, page 1. (https://www.gao.gov/assets/d24105563.pdf); "OAS Member States," *Organization of American States*, accessed August 12, 2024. (https://www.oas.org/en/member_states); "Charter of the Organization of American States," Bogota, April 30, 1948. (https://treaties.un.org/doc/Publication/UNTS/Volume%20119/volume-119-I-1609-English.pdf)

54. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=1382)

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

56. Ibid.

57. U.S. Department of Homeland Security, Press Release, “DHS Announces $18.2 Million In First-Ever Tribal Cybersecurity Grant Program Awards,” July 1, 2024. (https://www.dhs.gov/news/2024/07/01/dhs-announces-182-million-first-ever-tribal-cybersecurity-grant-program-awards)

58. Jonathan Greig, “CISA working on updated National Cyber Incident Response Plan,” *The Record*, October 23, 2023. (https://therecord.media/cisa-working-on-national-incident-response-plan)

59. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1267. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

60. Department of Defense, “National Defense Industrial Strategy,” November 16, 2023, pages 10, 17, and 23-24. (https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf)

61. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “National Cyber Incident Response Plan 2024,” October 2023, pages 1-2. (https://www.cisa.gov/sites/default/files/2023-10/NCIRP-2024-Fact-Sheet-508C.pdf)

62. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2059. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

63. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “FY 2025 Budget in Brief,” March 2024, page 106. (https://www.dhs.gov/sites/default/files/2024-03/2024_0311_fy_2025_budget_in_brief.pdf)

64. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4135. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=749)

65. Skylar Rispens, “National Guard ready to assist states with cyber response, say officials,” *StateScoop*, March 20, 2024. (https://statescoop.com/national-guard-ready-assist-with-state-cyber-response)

66. Maj. Benjamin Hughes, “National Guard Participates in Adriatic Cyber Exercise in Slovenia,” *U.S. Army*, July 10, 2024. (https://www.army.mil/article/277899/national_guard_participates_in_adriatic_cyber_exercise_in_slovenia)

67. Derek B. Johnson, “House Republicans propose eliminating funding for election security,” *CyberScoop*, June 5, 2024. (https://cyberscoop.com/house-republicans-propose-eliminating-funding-for-election-security); “Division B – Financial Services and General Government Appropriations Act, 2024,” *U.S. House of Representatives Document Repository*, March 18, 2024, page 28. (https://docs.house.gov/billsthisweek/20240318/Division%20B%20FSGG.pdf#page=29); “Explanatory Statement For Financial Services and General Government Appropriations Bill, 2023,” *U.S. Senate Committee on Appropriations*, accessed August 12, 2024, page 57. (https://www.appropriations.senate.gov/imo/media/doc/FSGGFY23RPT.pdf#page=57)

68. House Appropriations Committee, Appropriations Chairman Tom Cole, “Financial Services And General Government Appropriations Act, 2025,” June 3, 2024, page 5. (https://appropriations.house.gov/sites/evo-subsites/appropriations.house.gov/files/evo-media-document/fy25-fsgg-full-committee-bill-summary.pdf); Consolidated Appropriations Act, 2022, Pub. L. 117-103, 136 Stat 268. (https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf#page=220)

69. Financial Services and General Government Appropriations Act, 2025, 118th Congress (2024), page 76. (https://www.appropriations.senate.gov/imo/media/doc/FY25%20FSGG%20Bill%20Text%20-%20S4928RS-118.PDF)

70. Use of Campaign Funds for Candidate and Officeholder Security, U.S. Federal Election Commission, 11 Federal Register 24738, April 9, 2024. (https://www.federalregister.gov/documents/2024/04/09/2024-06863/use-of-campaign-funds-for-candidate-and-officeholder-security)

71. American Rescue Plan Act of 2021, Pub. L. 117-2, 135 Stat. 233. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=231); Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1267. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=839)

72. Colin Wood, “Kansas spends $2.8M on digital literacy training for underserved groups,” *StateScoop*, May 31, 2024. (https://statescoop.com/kansas-digital-literacy-skills-training-2024); Kansas Department of Commerce, “Kansas Department of Commerce; Broadband Update Testimony; Jade Piros de Carvalho, Director of Broadband; Senate Utilities Committee,” January 23, 2024, page 4. (https://kslegislature.org/li/b2023_24/committees/ctte_s_utils_1/documents/testimony/20240123_02.pdf)

73. Sophia Fox-Sowell, “California unlocks $70M for digital equity efforts,” *StateScoop*, April 5, 2024. (https://statescoop.com/california-gavin-newsom-70m-digital-equity-funding); California Department of Technology, “California Digital Equity Plan,” April 4, 2024, page 2. (https://broadbandforall.cdt.ca.gov/wp-content/uploads/sites/19/2024/04/California-State-Digital-Equity-Plan-04.04.2024-Remediated-Version.pdf)

74. U.S. Election Assistance Commission, “HAVA Grants Guidance: Using HAVA Funds to Combat AI-Generated Mis- and Disinformation,” March 21, 2024, page 1. (https://www.eac.gov/sites/default/files/2024-03/EAC_Guidance_on_Combatting_AI_Mis_%20and_Disinformation_03_21_24.pdf)

75. U.S. Federal Bureau of Investigation Director Christopher A. Wray, “Director Wray’s Remarks at the Intelligence and National Security Alliance Leadership Breakfast,” February 29, 2024. (https://www.fbi.gov/news/speeches/director-wray-s-remarks-at-the-intelligence-and-national-security-alliance-leadership-breakfast)

76. Martin Matishak, “Nakasone: 2024 will be most secure election ‘to date,’” *The Record*, January 31, 2024. (https://therecord.media/nakasone-nsa-cyber-command-election-will-be-secure)

77. Jonathan Greig, “FCC adopts voluntary ‘Cyber Trust Mark’ labeling rule for IoT devices,” *The Record*, March 14, 2024. (https://therecord.media/cyber-trust-mark-internet-of-things-devices-fcc-approval); Federal Communications Commission, “Notice of Proposed Rulemaking,” August 10, 2023. (https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf)

78. Jiwon Ma and Sophie McDowall, “Arming Consumers With Cybersecurity Data Can Protect U.S. Critical Infrastructure,” *Foundation for Defense of Democracies*, March 29, 2024. (https://www.fdd.org/analysis/policy_briefs/2024/03/29/arming-consumers-with-cybersecurity-data-can-protect-u-s-critical-infrastructure)

79. The White House, Press Release, “Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers,” July 18, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers)

80. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

81. John Sakellariadis, “Cyber world turns to S.F. confab,” *Politico*, April 24, 2023. (https://www.politico.com/newsletters/weekly-cybersecurity/2023/04/24/cyber-world-turns-to-s-f-confab-00093439); Jonathan Greig, “Bill proposes new DHS centers for testing security of critical government tech,” *The Record*, April 25, 2023. (https://therecord.media/dhs-cyber-testing-centers-bill-rep-ritchie-torres)

82. U.S. Department of Commerce, National Institute of Standards and Technology, “NIST Releases Version 2.0 of Landmark Cybersecurity Framework,” February 26, 2024. (https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework)

83. U.S. Department of Commerce, National Institute of Standards and Technology, “National Technical Information Service Fiscal Year 2025 Budget Submission to Congress,” March 2024, page 20. (https://www.commerce.gov/sites/default/files/2024-03/NIST-NTIS-FY2025-Congressional-Budget-Submission.pdf)

84. Sen. Angus King (R-ME) and Rep. Mike Gallagher (R-WI), “Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY21,” April 3, 2020, page 2. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy21); Reps. Jim Langevin (D-RI) and Mike Gallagher (R-WI), “Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY21,” March 13, 2020, page 2. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy21)

85. RADM (Ret.) Mark Montgomery and Michael Sugden, “Biden’s cybersecurity plan has a huge funding gap,” *The Hill*, May 8, 2024. (https://thehill.com/opinion/cybersecurity/4651731-bidens-cybersecurity-plan-has-a-huge-funding-gap)

86. The White House, “National Cybersecurity Strategy Implementation Plan,” July 2023, page 30. (https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf)

87. Suzanne Smalley, “Coker: ONCD is studying ‘liability regimes’ for software flaws,” *The Record*, February 7, 2024. (https://therecord.media/coker-oncd-studies-liability-regimes-for-software-bugs)

88. David DiMolfetta, “White House in talks with industry to build legal framework for software liability,” *NextGov*, May 6, 2024. (https://www.nextgov.com/cybersecurity/2024/05/white-house-talks-industry-build-legal-framework-software-liability/396330)

89. Kevin Poireault, “NIST National Vulnerability Database Disruption Sees CVE Enrichment on Hold,” *Infosecurity Magazine*, March 15, 2024. (https://www.infosecurity-magazine.com/news/nist-vulnerability-database)

90. U.S. Department of Commerce, National Institute of Standards and Technology, “NVD News,” July 2, 2024. (https://www.nist.gov/itl/nvd/nvd-news)

91. U.S. Department of Commerce, National Institute of Standards and Technology, “Statistics Results,” accessed August 12, 2024. (https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false)

92. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Extension of Comment Period, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 6 Federal Register 37141, May 6, 2024. (https://www.federalregister.gov/documents/2024/05/06/2024-09505/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements-extension-of)

93. Chris Jaikaran, “CIRCIA: Notice of Proposed Rule Making: In Brief,” *Congressional Research Service*, April 11, 2024, page 8. (https://sgp.fas.org/crs/misc/R48025.pdf)

94. The National Science And Technology Council, Cyber Security and Information Assurance Interagency Working Group, Networking and Information Technology Research and Development Subcommittee, “Federal Cybersecurity Research and Development Strategic Plan,” December 2023, pages 3 and 9. (https://www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf)

95. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “2024 JCDC Priorities,” accessed August 12, 2024. (https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities)

96. The White House, “National Cybersecurity Strategy Implementation Plan Version 2,” May 2024, page 43. (https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf)

97. U.S. National Science Foundation, “Dear Colleague Letter: IUCRC Proposals for Research and Thought Leadership on Insurance Risk Modeling and Underwriting Related to Terrorism and Catastrophic Cyber Risks: A Joint NSF and U.S. Department of the Treasury Federal Insurance Office Call,” April 24, 2024, pages 1-2. (https://www.nsf.gov/pubs/2024/nsf24082/nsf24082.pdf)

98. Natalie Alms, "Lawmakers try again with FISMA reform," *Nextgov/FCW*, March 7, 2024. (https://www.nextgov.com/cybersecurity/2024/03/lawmakers-try-again-fisma-reform/394780); John Hewitt Jones, "FISMA reform bill advances in Senate," *FedScoop*, July 26, 2023. (https://fedscoop.com/fisma-reform-bill-advances-in-senate)

99. U.S. Securities and Exchange Commission, Press Release, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," July 26, 2023. (https://www.sec.gov/news/press-release/2023-139)

100. FedRAMP, "A New Roadmap for FedRAMP," March 28, 2024. (https://www.fedramp.gov/2024-03-28-a-new-roadmap-for-fedramp)

101. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=844)

102. National Security Agency, Press Release, "NSA Releases Top Ten Cloud Security Mitigation Strategies," March 7, 2024. (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies)

103. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4777. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=1391); National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2042. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf#page=502)

104. Federal Communications Commission, "FCC Proposes Reporting Requirements Targeted to Improving Internet Routing Security," June 6, 2024, pages 1-2. (https://docs.fcc.gov/public/attachments/DOC-403034A1.pdf); Tim Starks, "FCC vote on tap for rules to secure fundamental component of the internet," *CyberScoop*, June 4, 2024. (https://cyberscoop.com/fcc-vote-on-tap-for-rules-to-secure-fundamental-component-of-the-internet)

105. Sara Friedman, "ONCD official highlights initiatives to improve government use of Border Gateway Protocol, memory safe programming," *Inside Cybersecurity*, June 27, 2024. (https://insidecybersecurity.com/daily-news/oncd-official-highlights-initiatives-improve-government-use-border-gateway-protocol)

106. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "FY 2025 Budget in Brief," March 2024, page 60. (https://www.dhs.gov/sites/default/files/2024-03/2024_0311_fy_2025_budget_in_brief.pdf)

107. "DOJ Leads Takedown of 'Likely the World's Largest Botnet Ever,'" *PYMNTS*, May 29, 2024. (https://www.pymnts.com/cybersecurity/2024/doj-leads-takedown-of-likely-the-worlds-largest-botnet-ever); U.S. Department of Justice, Office of Public Affairs, Press Release, "911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation," May 29, 2024. (https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation); Joshua Villanueva, "US Department of Justice dismantles massive botnet in major cybercrime crackdown," *JURISTNews*, May 31, 2024. (https://www.jurist.org/news/2024/05/us-department-of-justice-dismantles-massive-botnet-in-major-cybercrime-crackdown)

108. U.S. Department of Justice, Office of Public Affairs, "Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)," February 15, 2024. (https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian); U.S. Department of Justice, Office of Public Affairs, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," January 31, 2024. (https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical)

109. U.S. Department of Commerce, Bureau of Industry and Security Office of Technology Evaluation, "Assessment of the Status of the Microelectronics Industrial Base in the United States: A Study Conducted Under Section 705 of the Defense Production Act of 1950, As Amended," December 2023, page 76. (https://www.bis.doc.gov/index.php/documents/technology-evaluation/3402-section-9904-report-final-20231221/file)

110. U.S. Department of Defense, Press Release, "Department of Commerce and Department of Defense Sign Memorandum of Agreement to Strengthen U.S. Defense Industrial Base," July 26, 2023. (https://www.defense.gov/News/Releases/Release/Article/3470881/department-of-commerce-and-department-of-defense-sign-memorandum-of-agreement-t)

111. Executive Order 14017, "America's Supply Chain," February 24, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains)

112. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1478. (https://www.congress.gov/bill/117th-congress/house-bill/4346)

113. U.S. Department of Energy, "DOE Leads Effort to Improve the Cybersecurity of Energy Supply Chains," June 18, 2024. (https://www.energy.gov/articles/doe-leads-effort-improve-cybersecurity-energy-supply-chains); The White House, Press Release, "Fact Sheet: President Biden Announces New Actions to Strengthen America's Supply Chains, Lower Costs for Families, and Secure Key Sectors" November 27, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/27/fact-sheet-president-biden-announces-new-actions-to-strengthen-americas-supply-chains-lower-costs-for-families-and-secure-key-sectors)

114. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1576. (https://www.congress.gov/bill/117th-congress/house-bill/4346); Ibid., 136 Stat. 1584.

115. The White House, "Fact Sheet: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States," September 15, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states)

116. Cathleen D. Cimino-Isaacs and Karen M. Sutter, "The Committee on Foreign Investment in the United States," *Congressional Research Service*, May 17, 2024, page 2. (https://crsreports.congress.gov/product/pdf/IF/IF10177)

117. "Amendments to Penalty Provisions, Provision of Information, Negotiation of Mitigation Agreements, and Other Procedures Pertaining to Certain Investments in the United States by Foreign Persons and Certain Transactions by Foreign Persons Involving Real Estate in the United States," Department of the Treasury, Office of Investment Security, 31 Federal Register 26107, April 15, 2024. (https://www.federalregister.gov/documents/2024/04/15/2024-07693/amendments-to-penalty-provisions-provision-of-information-negotiation-of-mitigation-agreements-and)

118. U.S. Department of the Treasury, Press Release, "Treasury Issues Proposed Rule to Expand CFIUS Coverage of Real Estate Transactions Near Military Installations," July 8, 2024. (https://home.treasury.gov/news/press-releases/jy2449)

119. National Security Telecommunications Advisory Committee, "Measuring and Incentivizing the Adoption of Cybersecurity Best Practices," March 7, 2024, page 30. (https://www.cisa.gov/sites/default/files/2024-04/2024.03.07_NSTAC_M%26I_Report.pdf)

120. 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)

121. Hunton Andrews, "House Committee Postpones Markup Amid New Privacy Bill Updates," *The National Law Review*, July 3, 2024. (https://natlawreview.com/article/house-committee-postpones-markup-amid-new-privacy-bill-updates)

122. American Data Privacy and Protection Act, H.R.8152, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/house-bill/8152/text); Gregory T. Parks and Ronald W. Del Sesto, Jr., "US Data Privacy Legislation: Could a Federal Law be on the Horizon?" *Morgan Lewis*, July 31, 2023. (https://www.morganlewis.com/pubs/2023/07/us-data-privacy-legislation-could-a-federal-law-be-on-the-horizon)

123. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed August 12, 2024. (https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia); U.S. Securities and Exchange Commission, Press Release, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," July 26, 2023. (https://www.sec.gov/newsroom/press-releases/2023-139)

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

125. Ibid.

126. Ibid.

127. Office of the Inspector General of the Intelligence Community, "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 12, 2023, pages 20-23. (https://www.dni.gov/files/ICIG/Documents/News/ICIG%20News/2024/Joint_Report_on_the_Implementation_of_the_CISA_Act__of_2015_AUD-2023_002_Unclassified_Final_S_1.pdf)

128. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4094. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=708)

129. Grace Dille, "CISA Rolling out Joint Collaborative Environment to Enrich Threat Data," *MeriTalk*, July 17, 2023. (https://www.meritalk.com/articles/cisa-rolling-out-joint-collaborative-environment-to-enrich-threat-data)

130. Cate Burgan, "CISA Official: 'We Can't do Our Job Without Collaboration,'" *MeriTalk*, June 20, 2024. (https://www.meritalk.com/articles/cisa-official-we-cant-do-our-job-without-collaboration)

131. Cate Burgan, "CISA Taking $34M Budget Slash for FY2024," *MeriTalk*, March 22, 2024. (https://meritalk.com/articles/cisa-taking-34m-budget-slash-for-fy2024)

132. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2061. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

133. U.S. Cybersecurity and Infrastructure Security Agency Director Jen Easterly, "Opening Statement by CISA Director Jen Easterly," *Opening statement before the House Committee on Appropriations, Subcommittee on Homeland Security on the Fiscal Year 2025 Budget for the Cybersecurity and Infrastructure Security Agency*, April 30, 2024. (https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly-0)

134. U.S. House Committee on Appropriations, "Joint Explanatory Statement, Division Y—Cyber Incident Reporting for Critical Infrastructure Act of 2022," March 2022, page 2,524. (https://docs.house.gov/billsthisweek/20220307/BILLS-117HR2471SA-RCP-117-35.pdf)

135. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Extension of Comment Period, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 6 Federal Register 37141, May 6, 2024. (https://www.federalregister.gov/documents/2024/05/06/2024-09505/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements-extension-of)

136. Christian Vasquez, "Critical infrastructure organizations want CISA to dial back cyber reporting," *CyberScoop*, July 8, 2024. (https://cyberscoop.com/cisa-cyber-reporting-circia-2024)

137. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA Cybersecurity Strategic Plan 2024-2026," page 28. (https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf)

138. The White House, "National Cybersecurity Strategy Implementation Plan Version 2," May 2024, page 21. (https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf)

139. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4092. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=706)

140. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "FY 2025 Budget in Brief," March 2024, page 60. (https://www.dhs.gov/sites/default/files/2024-03/2024_0311_fy_2025_budget_in_brief.pdf)

141. Cate Burgan, "Easterly: China Threat Drives FY2025 Budget Boost Request," May 1, 2024. (https://www.meritalk.com/articles/easterly-china-threat-drives-fy2025-budget-boost-request); U.S. Cybersecurity and Infrastructure Security Agency Director Jen Easterly, "Opening Statement by CISA Director Jen Easterly," *Opening statement before the House Committee on Appropriations, Subcommittee on Homeland Security on the Fiscal Year 2025 Budget for the Cybersecurity and Infrastructure Security Agency*, April 30, 2024. (https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly-0)

142. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2039. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

143. U.S. Department of Defense, "Summary 2023 Strategy of Department of Defense," September 27, 2023, page 7. (https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF)

144. U.S. Department of Defense, "National Defense Industrial Strategy," November 16, 2023, page 27. (https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf)

145. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2032. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf); Ibid., 135 Stat. 2064.

146. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 566. and 137 Stat. 571. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf)

147. Mark Pomerleau, "Assessment for independent cyber force passes House, Senate defense committee," *DefenseScoop*, June 14, 2024. (https://defensescoop.com/2024/06/14/assessment-independent-cyber-force-passes-house-senate-defense-committee); National Defense Authorization Act for Fiscal Year 2025, S. 4638, 118th Congress (2024), Section 1606. (https://www.armed-services.senate.gov/imo/media/doc/fy25_ndaa_bill_text.pdf); National Defense Authorization Act for Fiscal Year 2025, H.R. 8070, 118th Congress (2024), Section 1536. (https://www.congress.gov/118/bills/hr8070/BILLS-118hr8070eh.pdf)

148. U.S. Department of Defense, the Office of the Under Secretary of Defense (Comptroller)/CFO, "Fiscal Year 2025 Budget Estimates United States Cyber Command," March 2024, page 9. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf)

149. Erica Lonergan and RADM (Ret.) Mark Montgomery, "United States Cyber Force: A Defense Imperative," *Foundation for Defense of Democracies*, March 2024. (https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf)

150. Mark Pomerleau, "Senate committee looks to withhold funding for Cybercom capability architecture," *DefenseScoop*, June 26, 2024. (https://defensescoop.com/2024/06/26/senate-committee-looks-to-withhold-funding-for-cybercom-capability-architecture)

151. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA Releases Malware Analysis Reports on Barracuda Backdoors," August 9, 2023. (https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors)

152. Cyber National Mission Force Public Affairs, "Cyber National Mission Force discloses IOCs from Ukrainian networks," U.S. Cyber Command, July 20, 2022. (https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks)

153. Cyber National Mission Force Public Affairs, "CYBERCOM's 'Under Advisement' to increase private sector partnerships, industry data-sharing in 2023," U.S. Cyber Command, June 29, 2023. (https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat); Martin Matishak, "As Cyber Command evolves, its novel malware alert system fades away," *The Record*, July 8, 2024. (https://therecord.media/cyber-command-virustotal-twitter-malware-alerts-cnmf)

154. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4080. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=694)

155. Ellen Nakashima, "White House authorizes 'offensive cyber operations' to deter foreign adversaries," *The Washington Post*, September 20, 2018. (https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html)

156. David Vergun, "Cybercom's Partnership With NSA Helped Secure U.S. Elections, General Says," *U.S. Department of Defense*, March 25, 2021. (https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says); NSA Public Affairs, Cyber National Mission Force Public Affairs, "How NSA, U.S. Cyber Command are defending midterm elections: One team, one fight," *U.S. National Security Agency*, August 25, 2022. (https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight)

157. Gen. Timothy D. Haugh, U.S. Cyber Command, "Posture Statement of General Timothy D. Haugh 2024," April 12, 2024. (https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024)

158. Chris Riotta, "US Cyber Command Expanded 'Hunt Forward' Operations in 2023," *Bank Info Security*, April 12, 2024. (https://www.bankinfosecurity.com/us-cyber-command-expanded-hunt-forward-operations-in-2023-a-24851); RADM (Ret.) Mark Montgomery and Annie Fixler, "Building Partner Capabilities for Cyber Operations," *Foundation for Defense of Democracies*, July 27, 2023. (https://www.fdd.org/wp-content/uploads/2023/07/fdd-memo-building-partner-capabilities-for-cyber-operations.pdf)

159. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 533. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=399)

160. National Defense Authorization Act for Fiscal Year 2020, Pub. L. 116-92, 133 Stat. 1747. (https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf#page=551)

161. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 567. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=433)

162. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 117-81, 135 Stat. 2028. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=426)

163. U.S. Cyber Command, "Academic Engagement," accessed August 15, 2024. (https://www.cybercom.mil/Partnerships-and-Outreach/Academic-Engagement)

164. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4087 and 134 Stat. 4140. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=701); National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2043, 135 Stat. 2054, and 135 Stat. 2093. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

165. Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021. (https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity); The White House, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems); Samantha Ravich and RADM (Ret.) Mark Montgomery, "Harden the cybersecurity of US nuclear complex now," *C4ISRNet*, October 26, 2022. (https://www.c4isrnet.com/thought-leadership/2022/10/26/harden-the-cybersecurity-of-us-nuclear-complex-now); James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136. Stat. 2940. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf#page=54

166. Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Activities, 89 Federal Register 17741, March 12, 2024. (https://www.federalregister.gov/documents/2024/03/12/2024-04752/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities)

167. "DC3 and DCSA Partner to Announce Vulnerability Disclosure Program for Defense Industrial Base," *Department of Defense Cyber Crime Center*, April 19, 2024. (https://content.govdelivery.com/accounts/USDODDC3/bulletins/39743d7)

168. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4130. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=744)

169. "New Solicitation Announcement," *U.S. Department of Defense, Defense Innovation Unit*, November 17, 2023. (https://diu.cmail20.com/t/j-e-sjiuluy-iijrikkilj-m)

170. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2046. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

171. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4109. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=723)

172. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 203. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=69)

173. National Defense Authorization Act for Fiscal Year 2025, H.R. 8070, 118th Congress (2024), Section 220b. (https://www.congress.gov/118/bills/hr8070/BILLS-118hr8070eh.pdf)

174. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

175. The White House, Press Release, "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers," July 18, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers)

176. Jonathan Greig, "FCC adopts voluntary 'Cyber Trust Mark' labeling rule for IoT devices," *The Record*, March 14, 2024. (https://therecord.media/cyber-trust-mark-internet-of-things-devices-fcc-approval); Federal Communications Commission, "Notice of Proposed Rulemaking," August 10, 2023. (https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf)

177. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, "FY24 Economic, High-Technology, White Collar, and Internet Crime Prevention National Training and Technical Assistance Program," June 6, 2024. (https://bja.ojp.gov/funding/opportunities/o-bja-2024-172174); U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, "BJA FY24 Economic, High-Technology, White Collar, and Internet Crime Prevention National Training and Technical Assistance Program," June 6, 2024, pages 3-6. (https://bja.ojp.gov/funding/O-BJA-2024-172174.pdf)

178. Further Consolidated Appropriations Act, 2024, H.R. 2882, 118th Congress (2024). (https://www.congress.gov/bill/118th-congress/house-bill/2882/text#H082E0B6446D24329841C455F099669A7#page=309)

179. "Collaborative Research: SaTC: CORE: Large: Rapid-Response Frameworks for Mitigating Online Disinformation," *U.S. National Science Foundation*, accessed August 15, 2024. (https://www.nsf.gov/awardsearch/showAward?AWD_ID=2120496&HistoricalAwards=false)

180. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3607. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf#page=1213)

181. The White House, Press Release, "Office of the National Cyber Director Announces Appointments Made Since its Establishment," August 30, 2022. (https://www.whitehouse.gov/oncd/briefing-room/2022/08/30/office-of-the-national-cyber-director-announces-appointments-made-since-its-establishment)

182. Further Consolidated Appropriations Act, 2024, H.R. 2882, 118th Congress (2024). (https://www.congress.gov/118/bills/hr2882/BILLS-118hr2882enr.pdf#page=75)

183. The White House, "FY 2025 Executive Office of the President Congressional Budget Submission," March 2024, page 57. (https://www.whitehouse.gov/wp-content/uploads/2024/03/FY-2025-Executive-Office-of-the-President-Congressional-Budget-Submission.pdf)

184. The White House, Press Release, "Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan," May 7, 2024 (https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2)

185. The White House, "M-24-14 Memorandum for the Heads of Executive Departments and Agencies," July 10, 2024, page 1. (https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf)

186. The White House, Office of the National Cyber Director, "National Cyber Workforce and Education Strategy Initial Stages of Implementation," June 25, 2024, page 2. (https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

187. The White House, Press Release," National Cyber Director Encourages Adoption of Skill-Based Hiring to Connect Americans to Good-Paying Cyber Jobs," April 29, 2024. (https://www.whitehouse.gov/oncd/briefing-room/2024/04/29/press-release-wh-cyber-workforce-convening); Elias Groll, "White House moves to ease education requirements for federal cyber contracting jobs," *CyberScoop*, January 11, 2024. (https://cyberscoop.com/harry-coker-education-requirements-federal-cybersecurity-jobs)

188. Assistant National Cyber Director Seeyew Mo, "Hearing on 'Finding 500,000: Addressing America's Cyber Workforce Gap,'" *Testimony before Committee on Homeland Security*, June 26, 2024, page 2. (https://homeland.house.gov/wp-content/uploads/2024/06/2024-06-26-HRG-Testimony.pdf)

189. The White House, "Fact Sheet: President Biden Signs Executive Order: Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums," March 6, 2024. (https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/06/fact-sheet-president-biden-signs-executive-order-scaling-and-expanding-the-use-of-registered-apprenticeships-in-industries-and-the-federal-government-and-promoting-labor-management-forums)

190. U.S. Department of Labor, Press Release, "Biden-Harris Administration Announces Nearly $200m Available in Grants to Expand Registered Apprenticeships," February 21, 2024. (https://www.dol.gov/newsroom/releases/eta/eta20240221)

191. The White House, Office of the National Cyber Director, "National Cyber Workforce and Education Strategy Initial Stages of Implementation," June 25, 2024, page 5. (https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

192. U.S. Department of Education, Press Release, "U.S. Department of Education Announces Key K-12 Cybersecurity Resilience Efforts," August 7, 2023. (https://www.ed.gov/news/press-releases/department-of-education-announces-k-12-cybersecurity-resilience-efforts)

193. U.S. Department of Education, Press Release, "U.S. Department of Education Launches Government Coordinating Council to Strengthen Cybersecurity in Schools," March 28, 2024. (https://www.ed.gov/news/press-releases/us-department-education-launches-government-coordinating-council-strengthen-cybersecurity-schools)

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

195. The White House, Office of the National Cyber Director, "National Cyber Workforce and Education Strategy Initial Stages of Implementation," June 25, 2024, page 5. (https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

196. "Investing in America's cybersecurity workforce," *Google*, accessed August 15, 2024. (https://cyberclinics.withgoogle.com)

197. Natalie Alms, "OPM pitches Congress on a federal cyber workforce revamp," *NextGov/FCW*, March 19, 2024. (https://www.nextgov.com/cybersecurity/2024/03/opm-pitches-congress-federal-cyber-workforce-revamp/395067)

198. U.S. Office of Personnel Management, "Action Plan for Strengthening Officer Recruitment, Hiring, Promotion, and Retention," October 2023, pages 2 and 11. (https://www.opm.gov/policy-data-oversight/hiring-information/reports/action-plan-for-strengthening-officer-recruitment-hiring-promotion-and-retention.pdf)

199. U.S. Office of Personnel Management, "Pay Flexibility, Incentive Pay, and Leave and Workforce Flexibility Programs for Artificial Intelligence (AI), AI-enabling, and Other Key Technical Employees," February 27, 2024. (https://www.chcoc.gov/content/pay-flexibility-incentive-pay-and-leave-and-workforce-flexibility-programs-artificial)

200. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1530. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf#page=166)

201. Executive Order 14035, "Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce," June 25, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce)

202. Elias Groll, "White House moves to ease education requirements for federal cyber contracting jobs," *CyberScoop*, January 11, 2024. (https://cyberscoop.com/harry-coker-education-requirements-federal-cybersecurity-jobs)

203. The White House, "Fact Sheet: Biden-Harris Administration Highlights New Commitments Toward Equitable Workforce Development in Advanced Manufacturing," January 23, 2024. (https://www.whitehouse.gov/briefing-room/statements-releases/2024/01/23/fact-sheet-biden-harris-administration-highlights-new-commitments-toward-equitable-workforce-development-in-advanced-manufacturing)

204. The White House, Press Release, "National Cyber Director Encourages Adoption of Skill-Based Hiring to Connect Americans to Good-Paying Cyber Jobs," April 29, 2024. (https://www.whitehouse.gov/oncd/briefing-room/2024/04/29/press-release-wh-cyber-workforce-convening)

205. Federal Cyber Workforce Training Act of 2024, S. 4715, 118th Congress (2024). (https://www.congress.gov/bill/118th-congress/senate-bill/4715/text)

206. Weslan Hansen, "Bill to Create Federal Cyber Workforce Institute Passes Senate Panel," *Meritalk*, August 1, 2024. (https://meritalk.com/articles/senate-bill-aims-to-create-federal-cyber-workforce-institute)

207. Maureen Dunne, "Building the Neurodiversity Talent Pipeline for the Future of Work," *MIT Sloan Management Review*, November 28, 2023. (https://sloanreview.mit.edu/article/building-the-neurodiversity-talent-pipeline-for-the-future-of-work)

208. The White House, Office of the National Cyber Director, "National Cyber Workforce and Education Strategy Initial Stages of Implementation," June 25, 2024, page 4. (https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

209. "NIST Awards $3.6 Million for Community-Based Cybersecurity Workforce Development," *U.S. Department of Commerce, National Institute of Standards and Technology*, April 3, 2024. (https://www.nist.gov/news-events/news/2024/04/nist-awards-36-million-community-based-cybersecurity-workforce-development)

210. Executive Order 14017, "Executive Order on America's Supply Chains," February 24, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains)

211. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "CISA Announces Renewal of Information and Communications Technology Supply Chain Risk Management Task Force," February 6, 2024. (https://www.cisa.gov/news-events/news/cisa-announces-renewal-information-and-communications-technology-supply-chain-risk-management-task)

212. U.S. Department of Homeland Security, U.S. Department of Commerce, "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," February 24, 2022. (https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf)

213. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1642. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf#page=278); "Find Potential NSF Engines," U.S. National Science Foundation, accessed August 15, 2024. (https://new.nsf.gov/funding/initiatives/regional-innovation-engines/find-potential-nsf-engines)

214. The White House, "Fact Sheet: Biden-Harris Administration Announces 31 Regional Tech Hubs to Spur American Innovation, Strengthen Manufacturing, and Create Good-Paying Jobs in Every Region of the Country," October 23, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/23/fact-sheet-biden-harris-administration-announces-31-regional-tech-hubs-to-spur-american-innovation-strengthen-manufacturing-and-create-good-paying-jobs-in-every-region-of-the-country)

215. The White House, "Fact Sheet: Biden-Harris Administration Announces Investment in Twelve Regional Technology Hubs Creating Good-Paying Jobs and Driving Economic Opportunity and Innovation in Communities Across the Country," July 2, 2024. (https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/02/fact-sheet-biden-harris-administration-announces-investment-in-twelve-regional-technology-hubs-creating-good-paying-jobs-and-driving-economic-opportunity-and-innovation-in-communities-across-the-cou)

216. U.S. Department of Commerce, "Fact Sheet: Biden-Harris Administration Announces Over $5 Billion in CHIPS and Science Act Funding to Spur Domestic Semiconductor Manufacturing and Innovation," February 9, 2024. (https://www.commerce.gov/news/fact-sheets/2024/02/fact-sheet-biden-harris-administration-announces-over-5-billion-chips-and)

217. "CHIPS Incentives Awards," *U.S. Semiconductor Industry Association*, August 6, 2024. (https://www.semiconductors.org/chips-incentives-awards)

218. U.S. Department of Defense, "FY24 Investment Strategy for the Office of Strategic Capital," March 9, 2024, page 1. (https://media.defense.gov/2024/Mar/09/2003409961/-1/-1/0/FY24-INVESTMENT-STRATEGY-FOR-THE-OFFICE-OF-STRATEGIC-CAPITAL-DISTRIBUTION-STATEMENT-A-%20APPROVED-FOR-PUBLIC-RELEASE.PDF); Sandra Erwin, "DoD Unveils Investment Strategy for Its Office of Strategic Capital," *Space News*, March 11, 2024. (https://spacenews.com/dod-unveils-investment-strategy-for-its-office-of-strategic-capital)

219. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4768–4773. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf#page=1382); "Sector Risk Management Agencies," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed August 15, 2024. (https://www.cisa.gov/stopransomware/sector-risk-management-agencies)

220. "Supply Chain Optimization and Intelligence Network Celebrates First Anniversary," *U.S. Department of Commerce, National Institute of Standards and Technology*, May 29, 2024. (https://www.nist.gov/news-events/news/2024/05/supply-chain-optimization-and-intelligence-network-celebrates-first)

221. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

222. Jonathan Greig, "Bill proposes new DHS centers for testing security of critical government tech," *The Record*, April 25, 2023. (https://therecord.media/dhs-cyber-testing-centers-bill-rep-ritchie-torres)

223. U.S. Department of Defense, "Emerging Mid-Band Radar Spectrum Sharing (EMBRSS) Feasibility Assessment Report," September 2023, pages 10-11. (https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-EMBRSS-FeasabilityAssessmentRedacted.pdf)

224. U.S. Department of Commerce, National Telecommunications and Information Administration, "National Spectrum Strategy," November 2023, page 8. (https://www.ntia.gov/sites/default/files/publications/national_spectrum_strategy_final.pdf)

225. U.S. Department of Commerce, National Telecommunications and Information Administration, Press Release, "Biden-Harris Administration Announces $420M Funding Opportunity to Promote Wireless Innovation," July 9, 2024. (https://www.ntia.gov/press-release/2024/biden-harris-administration-announces-420m-funding-opportunity-promote-wireless)

226. Maggie Miller, "U.S. Cyber Ambassador to Push Pacific Allies to Step Up Undersea Cable Security," *Politico*, January 29, 2024. (https://subscriber.politicopro.com/article/2024/01/us-cyber-ambassador-to-push-pacific-allies-to-step-up-undersea-cable-security-00138352)

227. The White House, "United States-Australia Joint Leaders' Statement: Building an Innovation Alliance," October 25, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/25/united-states-australia-joint-leaders-statementbuilding-an-innovation-alliance)

228. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1372. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf)

229. "EXIM Announces Longer Repayment Terms, Flexibilities for Climate Projects," *U.S. Export-Import Bank*, July 12, 2023. (https://www.exim.gov/news/exim-announces-longer-repayment-terms-flexibilities-for-climate-projects)

230. Export-Import Bank Act of 1945, Pub. L. 79-173, codified as amended at 12 U.S.C. §§635. (https://img.exim.gov/s3fs-public/21-01-19-exim-bank-2019-charter-as-amended-final.pdf)

231. "About Us," *U.S. Trade and Development Agency*, accessed August 15, 2024. (https://www.ustda.gov/about)

232. U.S. Senate Committee on Commerce, Science, and Transportation, Press Release, "Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation," April 7, 2024. (https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation)

233. iCivics, "Press Release: Funding for Civic Education Remains Flat as Congress Passes Fiscal Year 2024 Budget, But Civxnow Looks Toward Future," March 25, 2024. (https://civxnow.org/press-release-funding-for-civic-education-remains-flat-as-congress-passes-fiscal-year-2024-budget-but-civxnow-looks-toward-future); American History and Civics National Academies received $3 million and American Civics National Activities received $20 million in a competitive grant program. See: U.S. Senate Committee on Appropriations, "Division H - Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2023," page 236. (https://www.appropriations.senate.gov/imo/media/doc/Division%20H%20-%20LHHS%20Statement%20FY23.pdf)

234. U.S. Department of Education, "Fiscal Year 2025 Budget Summary," March 2024, page 74. (https://www2.ed.gov/about/overview/budget/budget25/summary/25summary.pdf)

235. FederalGrantsWire, "American History and Civics Education," 2024. (https://www.federalgrantswire.com/american-history-and-civics-education.html); iCivics, "Press Release: Funding for Civic Education Remains Flat as Congress Passes Fiscal Year 2024 Budget, But Civxnow Looks Toward Future," March 25, 2024. (https://civxnow.org/press-release-funding-for-civic-education-remains-flat-as-congress-passes-fiscal-year-2024-budget-but-civxnow-looks-toward-future)

236. U.S. House of Representatives, "The Weaponization of the National Science Foundation: How NSF Is Funding the Development of Automated Tools to Censor Online Speech 'At Scale' and Trying to Cover Up Its Actions," February 5, 2024. (https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/NSF-Staff-Report_Appendix.pdf)

237. U.S. Department of State, "The Framework to Counter Foreign State Information Manipulation," January 18, 2024. (https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation)

238. U.S. Department of State, U.S. Embassy in Burkina Faso, "Funding Opportunity – Global Engagement Center Public Diplomacy Small Grant," April 29, 2024. (https://bf.usembassy.gov/funding-opportunity-global-engagement-center-public-diplomacy-small-grant); U.S. Department of State, "Congressional Budget Justification Foreign Operations Appendix 2, Fiscal Year 2025," page 307. (https://www.state.gov/wp-content/uploads/2024/03/State-and-USAID-Appendix-2.pdf)

239. U.S. Secretary of State Antony Blinken, *Opening Remarks Before the House Committee on Foreign Affairs on the FY25 Department of State Budget Request*, May 22, 2024. (https://www.state.gov/opening-remarks-before-the-house-committee-on-foreign-affairs-on-the-fy25-department-of-state-budget-request)

240. U.S. Department of Homeland Security, Press Release, "Following HSAC Recommendation, DHS terminates Disinformation Governance Board," August 24, 2022. (https://www.dhs.gov/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board)

241. Will Oremus, "GOP: Biden violated First Amendment by pressing Big Tech on covid misinfo," *The Washington Post*, June 21, 2023. (https://www.washingtonpost.com/technology/2023/06/21/gop-biden-covid-misinfo-censorship)

242. Sara Friedman and Jacob Livesay, "Easterly praises Supreme Court decision on government interactions with social media companies," *Inside Cybersecurity*, June 28, 2024. (https://insidecybersecurity.com/daily-news/easterly-praises-supreme-court-decision-government-interactions-social-media-companies)

243. U.S. Department of Homeland Security, Federal Emergency Management Agency, "The U.S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Homeland Security Grant Program," April 16, 2024. (https://www.fema.gov/grants/preparedness/homeland-security/fy-24-nofo)

244. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Enhancing Election Security Through Public Communications," May 2024, page 3. (https://www.cisa.gov/sites/default/files/2024-06/Enhancing%20Election%20Security%20Through%20Public%20Communications_508c.pdf)

245. PAID OFF Act of 2023, S. 434, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/senate-bill/434/text); Disclosing Foreign Influence in Lobbying Act, S. 829, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/senate-bill/829)

246. Brian D. Smith and Alex Langton, "Congress Removes Foreign Agents Registration Act ('FARA')-Related Provisions from Final NDAA," *Covington*, December 7, 2023. (https://www.insidepoliticallaw.com/2023/12/07/congress-removes-foreign-agents-registration-act-fara-related-provisions-from-final-ndaa)

247. Providing for Consideration of the Bill (H.R. 8070) to Authorize Appropriations for Fiscal Year 2025 for Military Activities, H. Rept. 118-551, 118 Congress (2024). (https://www.congress.gov/congressional-report/118th-congress/house-report/551)

248. House Appropriations Committee, Appropriations Chairman Tom Cole, Press Release, "Committee Approves FY25 Homeland Security Appropriations Act," June 12, 2024. (https://appropriations.house.gov/news/press-releases/committee-approves-fy25-homeland-security-appropriations-act)

249. Protecting Americans from Foreign Adversary Controlled Applications Act, H.R.7521, 118th Congress (2024). (https://www.congress.gov/bill/118th-congress/house-bill/7521)

About the Authors

Jiwon Ma is a senior program analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. Jiwon received a Master of International Affairs degree from Columbia University's School of International and Public Affairs and a B.A. in global studies from Lesley University.

RADM (Ret.) Mark Montgomery serves as senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Mark also directs CSC 2.0 — a project established to continue the work of the Cyberspace Solarium Commission — having served as the commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee under the leadership of Senator John S. McCain, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

ACKNOWLEDGEMENTS

The authors of the CSC 2.0 Annual Assessment report would like to express their gratitude toward the co-chairs and advisors for providing their valuable expertise and advice in carrying forward the work of the Cyberspace Solarium Commission. The commission's effectiveness stemmed from their innovative ideas and unwavering commitment to implementing effective policies. We extend our gratitude to Annie Fixler for her exceptional editorial and organizational skills in ensuring the successful launch of the publication. We are also grateful to David Adesnik and David May for their unparalleled editing skills. While many experts helped refine the assessment, any errors in fact or judgment are ours alone. Finally, we would like to thank Erin Blumenthal, Daniel Ackerman, and Pavak Patel of the Foundation for Defense of Democracies for bringing this report to life through data visualizations and design.

Cover Photo: Senator Angus King and Representative Mike Gallagher speak at event hosted by the Foundation for Defense of Democracies on September 19, 2023. (Photo by Jeff Song/FDD)

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partner

FDD

CSC 2.0

Preserving and Continuing the
Cyberspace Solarium Commission