CSC 2.0

October 2025

2025 Annual Report on Implementation

Jiwon Ma

Table of Contents

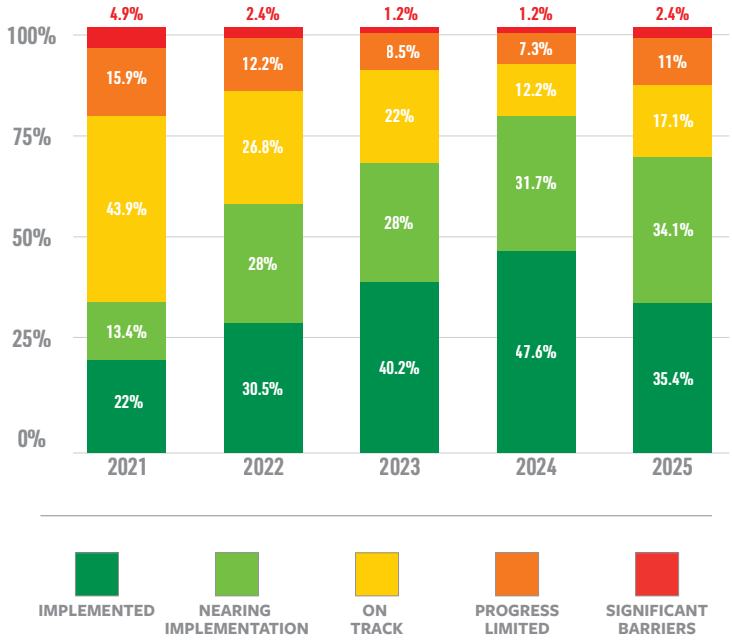
Executive Summary

Our nation's ability to protect itself and its allies from cyber threats is stalling and, in several areas, slipping. For five years, the U.S. Cyberspace Solarium Commission's (CSC's) recommendations have served as a benchmark against which to measure policymakers' commitment to strengthening the nation's cybersecurity. This report assesses that approximately 35 percent of the commission's original 82 recommendations have been fully implemented, 34 percent are nearing implementation, and an additional 17 percent are on track to be implemented. By comparison, however, last year's report concluded that 48 percent had been implemented, 32 percent were nearing implementation, and an additional 12 percent were on track. For the first time, there has been a substantial reversal of the advances made in previous years. Nearly a quarter of fully implemented recommendations have lost that status — an unprecedented setback that underscores the fragility of progress.

Indeed, implementation alone does not guarantee institutional durability; key reforms remain vulnerable to underinvestment or bureaucratic gridlock that slows or prevents new initiatives from taking root. Personnel turnover and shifts in priorities during presidential transitions have historically also slowed cybersecurity progress. This year's assessment makes clear that technology is evolving faster than federal efforts to secure it. Meanwhile, cuts to cyber diplomacy and science programs and the absence of stable leadership at key agencies like the Cybersecurity and Infrastructure Agency (CISA), the State Department, and the Department of Commerce have further eroded momentum.

Implementation of any one set of recommendations is insufficient on its own to deter, thwart, or mitigate malign cyber activities. Rather, the Cyberspace Solarium Commission designed a new strategic approach — layered cyber deterrence — to reduce the likelihood and impact of significant cyberattacks.

Progress Toward Implementation of the March 2020 Recommendations



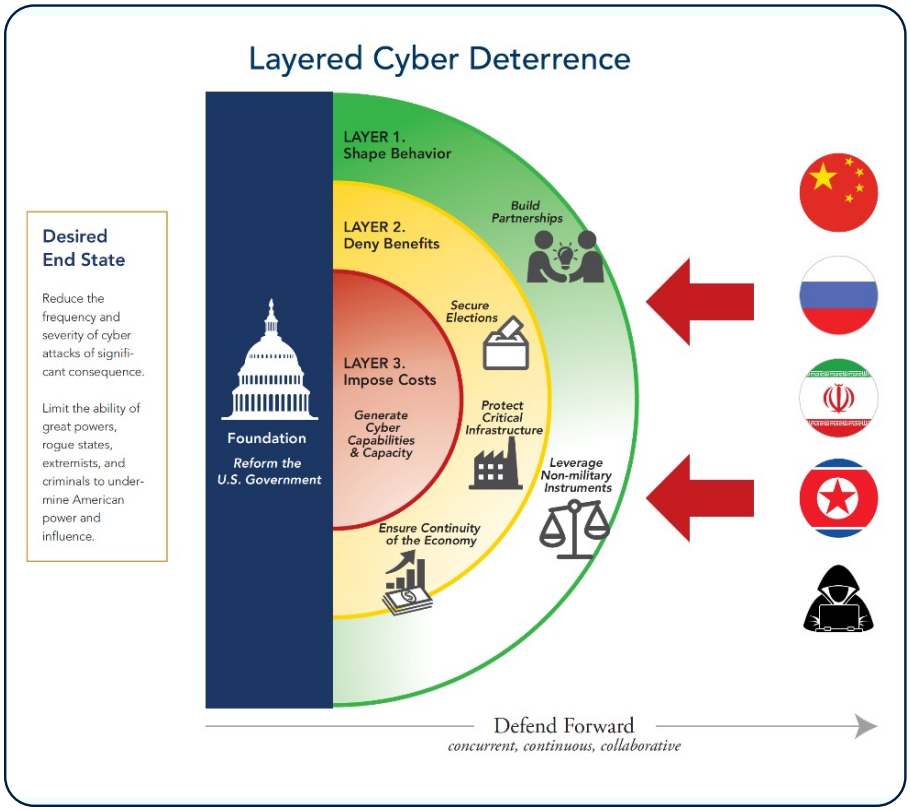
Indeed, many of Washington's most important policy choices have reflected the commission's strategy of layered cyber deterrence — the government has been shaping the behavior of foreign states while denying benefits and imposing costs on those who threaten democratic values in cyberspace. In some cases, this is directly through implementation of CSC recommendations; in others, it is indirectly through alignment with the CSC framework. Congressional and White House action have strengthened U.S. cyber resilience by expanding institutional capacity, improving interagency collaboration, and deepening public-private collaboration. But more work must be done.

Shaping behavior. The State Department's Bureau of Cyberspace and Digital Policy (CDP) plays a critical role in promoting responsible state behavior in international forums. Led by an ambassador-at-large, CDP is uniquely positioned to advance U.S. security and economic interests abroad, enabling federal agencies to focus on strengthening cyber resilience at home. The bureau needs a Senate-confirmed leader to be most effective.

Denying benefits. A successful whole-of-nation approach to deterring adversaries requires strong industry partnerships and stable Senate-confirmed leaders to carry out the mission. The Office of the National Cyber Director (ONCD) has driven strategic alignment across the federal enterprise, while CISA has deepened engagement with critical infrastructure owners and operators and state, local, tribal, and territorial governments. Maintaining these partnerships has been challenging as contract lapses and the weakening of liability protections have strained trust. Private capital continues

to reinforce these partnership efforts through initiatives such as Cyber Clinics that support both victims of cyberattacks as well as research and development programs that drive innovation.

Imposing costs. U.S. law enforcement agencies and the Department of Defense (DOD) have reinforced deterrence by working with allies and partners to conduct persistent engagement and take down botnets before they reach U.S. networks. But attacks continue, indicating our adversaries are not being forced to bear sufficient costs for their malign activities.



Source: Cyberspace Solarium Commission

What began as a forward-looking vision has become an urgent set of unfinished tasks. The challenge is to reinforce what has been built and address the gaps that remain. That requires a national cyber director with real budget and authority; empowering CISA and sector risk management agencies; restoring diplomatic tools and foreign assistance to extend U.S. reach abroad; and ensuring the cyber workforce can meet tomorrow's challenges. Building a more robust domestic response capacity is also becoming a clear need. Lastly, achieving these goals will require reestablishing bipartisan consensus on cybersecurity as a core element of national security.

The United States faces a pivotal decision point. It is up to the administration and Congress to seize this opportunity to secure the gains of the past five years; reinforce its cyber deterrence posture; and send a clear signal of capability, intent, and continuity to its adversaries.

Senator Angus King (advisory)
Former Chairman of the
Cyberspace Solarium Commission

Top 5 Recommendations for the Trump Administration and Congress

Over the past five years, the Cyberspace Solarium Commission helped lay the foundation for stronger U.S. cyber policy, spurring real progress across government and industry. Yet weak statutory authorities, diminished diplomatic capacity, and growing workforce and regulatory gaps continue to threaten national resilience. Addressing these challenges will require action from both Congress and the administration. The following five priorities mark the next phase in strengthening America's cyber defense in the years ahead.

1. Enhance the Authorities of the Office of the National Cyber Director

The ONCD, created in the fiscal year (FY) 2021 National Defense Authorization Act (NDAA),[1] has grown into a permanent fixture of U.S. cyber governance. Although the office has proven effective at convening agencies and shaping strategy, it still lacks the positional authority and interagency relationships needed to enforce decisions across the government. This gap undermines efficiency and slows progress on urgent tasks. The same is true for resources: ONCD can review agency budget submissions but has no authority to align cyber investments across departments, leaving federal resources missing, fragmented, or duplicative. Regulatory oversight presents similar challenges. Without a mandate to harmonize regulations, ONCD cannot resolve the patchwork of conflicting requirements facing critical infrastructure operators, a problem that industry has repeatedly warned is eroding trust in government guidance.[2] To address these shortcomings, the ONCD should lead efforts to rewrite the decade-old policy document, known as Presidential Policy Directive 41,[3] to clarify responsibilities for the national incident response process. President Donald Trump should issue an executive order to grant ONCD formal convening authority over civilian agency cyber policy, review authority over agency cyber budgets, and a mandate to lead regulatory harmonization efforts through an interagency working group. Elevating ONCD's role with these actions would provide the clarity and authority needed for ONCD to fulfill its role as the central driver of national cyber policy.

2. Restore the Workforce and Funding of the Cybersecurity and Infrastructure Security Agency

CISA is the federal government's cyber defense agency, responsible for leading national incident response, issuing threat advisories, and developing resilience programs across sectors. National Security Memorandum 22 reaffirmed this role, designating CISA as the national coordinator for the security and resilience of critical infrastructure.[4] Yet CISA's effectiveness has been weakened by steep workforce and budget cuts that undermine its ability to support operators on the ground. These pressures limit CISA's ability to scale critical programs that give the administration early visibility into attacks and to share information with private sector partners. By investing in CISA in its role as national coordinator, the administration can prevent disruptions, protect American families, and ensure economic stability. The administration should develop a plan of action and restore staffing and budget levels, with the goal of establishing and reinforcing CISA's role as national coordinator for the security and resilience of critical infrastructure.[5] Congress should provide multiyear funding stability to prevent further erosion of capacity. Empowering CISA strengthens the administration's hand in deterring adversaries and demonstrates visible leadership in keeping the country safe.

3. Restore Funding and Personnel Dedicated to Cyber Diplomacy and Capacity Building at the State Department

Congress codified the State Department's CDP with the Cyber Diplomacy Act of 2022. CDP's mission is to strengthen capacity and confidence among allies and partners.[6] Since its codification, CDP has developed key strategies and led engagements with partners — from standing up incident response capabilities to jointly countering authoritarian narratives online. CDP leveraged a dedicated cyber-assistance fund to help nations rapidly mitigate attacks and paired U.S. seed funding with allied and private-sector investment to crowd out Chinese firms seeking to dominate telecommunications and emerging technology supply chains.[7] However, CDP's effectiveness has been constrained by a restructuring effort that fractured cyber expertise across the State Department and stripped away resources that would allow the bureau to coordinate policy and programs effectively, reducing available partner cyber capacity funds. Meanwhile, adversaries like China continue to expand their global digital influence and dominate international technical standard-setting bodies, filling the vacuum left by U.S. retrenchment. The administration should restore CDP's personnel and resources through reprogramming, supplemental requests, or executive orders, while Congress complements this effort by creating a

long-term funding line that ensures the continuity of cyber-capacity building programs. To rebuild trust, the Trump administration must demonstrate to allies that Washington is a reliable partner in building secure digital infrastructure that supports U.S. trade and investment.

4. Maintain and Restore Critical Support to Public Collaboration Effort

The Critical Infrastructure Partnership Advisory Council (CIPAC) has provided a legal framework for information exchange between the federal government and private-sector partners for nearly two decades. The Trump administration's decision to eliminate CIPAC[8] created legal uncertainty around information sharing, undermining long-standing trust between industry and government. Since its elimination, critical infrastructure operators have scaled back their engagement with the federal government out of concern that sensitive company data could be publicly exposed.[9] If the Department of Homeland Security (DHS) fails to immediately reinstate CIPAC, Congress should intervene to restore clear legal protections for industry-government dialogue. Congress should also pass a long-term reauthorization of existing cybersecurity information sharing protections.

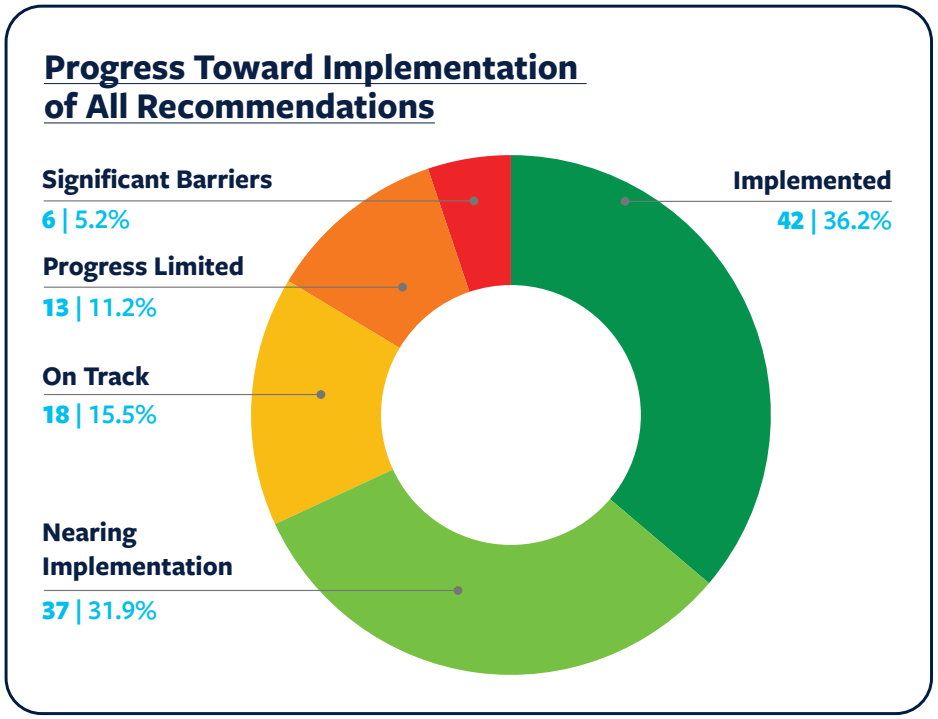
5. Expand the Talent Pool and Improve Retention of the Cyber Workforce

Since the start of the Trump administration, several workforce decisions have reshaped how the federal government recruits and retains cyber talent. New hiring practices and at-will mandates shift emphasis away from technical qualifications and discourage qualified candidates from pursuing career roles. The rollback of diversity, equity, and inclusion initiatives eliminated programs that had broadened the pipeline of skilled candidates from underrepresented and nontraditional backgrounds, narrowing access to key talent pools. The result is a growing gap in filling critical cyber positions from an already limited talent pool. While the administration has wisely called for both "skills-based" and "merit-based" hiring, it has yet to establish a consistent workforce model to deliver on those goals — risking what had been a rare area of bipartisan consensus around building a skills-based cyber workforce.[10] Clarifying a consistent, skills-based model — and broadening the pipelines for nontraditional candidates through apprenticeships, training, and scholarship-for-service programs — will be essential to stabilizing the cyber workforce and ensuring agencies have the expertise to defend the nation's most critical systems. Also, the government should expand proven skills-based recruitment programs like CyberCorps.

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.[11] This report is the fifth 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. 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.



Implementation Status	
	Implemented: The recommendation was included in legislation that 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: The recommendation is not expected to move in the immediate future but is 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	2025
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	Reestablish 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: The March 2023 National Cybersecurity Strategy issued by the Biden administration remains nominally in effect as the governing document for federal cybersecurity policy. As the Trump administration develops its own national security and national cybersecurity strategies, the administration should ensure cybersecurity remains a central component of national security planning, reaffirm federal roles and responsibilities, and set well-defined priorities for critical infrastructure protection.

1.1.1 — Develop a Multitiered Signaling Strategy: Effective deterrence requires consistent, credible signaling that can endure leadership changeovers. In the first months of the Trump administration, Defense Secretary Pete Hegseth reportedly ordered U.S. Cyber Command to pause offensive operations against Russia during sensitive negotiations,[12] despite ongoing Russian cyber activity. The Pentagon has denied these reports,[13] but early moves by the administration indicated it would not treat Russia as a cyber threat[14] — a shift that could undermine U.S. deterrence.

1.1.2 — Promulgate a New Declaratory Policy: A clear declaratory policy that signals the costs of malicious cyber activity is essential for deterring adversaries. The Trump administration entered office declaring that Washington needed to go on offense to punish Chinese hackers for attacks on U.S. critical infrastructure. Since then, the administration has continued to use law enforcement tools and financial sanctions to punish China's malicious cyber activity.[15]

1.2 — Create House Permanent Select and Senate Select Committees on Cybersecurity: Congress has shown no appetite for consolidating jurisdiction over cybersecurity into a single committee in either chamber. Existing committee structures remain fragmented, with overlapping and sometimes competing jurisdictions that hinder effective oversight.

1.2.1 — Reestablish the Office of Technology Assessment: Congress continues to rely on the Government Accountability Office and Congressional Research Service to fill the Office of Technology Assessment's role rather than reestablishing it. However, this workaround remains inadequate. As noted in previous annual assessments, Congress has failed to build the internal capacity needed to meet growing demand for technical expertise on complex cybersecurity issues.

1.3 — Establish a National Cyber Director Position: The Senate confirmed Sean Cairncross on August 2, 2025, as the third national cyber director, succeeding Harry Coker Jr.[16]

1.4 — Strengthen the Cybersecurity and Infrastructure Security Agency: The Trump administration's FY26 budget proposed a nearly 17 percent cut to CISA's budget.[17] In addition, the White House has proposed cutting about a third of its workforce,[18] and the secretary of homeland security has allowed multiple contracts to lapse, further shrinking CISA's technical and outreach resources.[19] While the House Appropriations Committee approved a $2.7 billion budget for the agency, representing only a 5 percent cut,[20] CISA has reduced capabilities at a time when its mission is more critical than ever.

1.4.1 — Codify and Strengthen the Cyber Threat Intelligence Integration Center: The Biden administration reestablished the Cyber Threat Intelligence Integration Center (CTIIC) at the Office of the Director of National Intelligence (ODNI) in FY22. However, in August 2025, Director of National Intelligence Tulsi Gabbard announced the formal shutdown of CTIIC as part of the "ODNI 2.0" restructuring plan, which includes a 40 percent cut to ODNI staff.[21] CTIIC's closure leaves a major gap in the government's ability to coordinate cyber intelligence at scale. It ends key programs like the Critical Infrastructure Intelligence Initiative, which provided monthly classified briefings to critical infrastructure owners and operators.[22] The shutdown disrupts real-time cyber threat information sharing between the federal government and private sector.

1.4.2 — Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force: The National Cyber Investigative Joint Task Force (NCIJTF) remains the federal government's lead cyber threat response center,[23] bringing together personnel from more than 30 federal agencies to deliver coordinated, multi-agency cyber threat intelligence.[24] A September 2024 Justice Department audit called for clearer roles and stronger performance metrics — particularly for the Criminal Mission Center within NCIJTF[25] — but the FBI has since demonstrated meaningful progress. In 2024 alone, the bureau conducted over 30 operations disrupting ransomware groups,[26] reflecting improved coordination, tracking, and mission focus. NCIJTF also responded to new challenges, partnering with CISA and the National Security Agency during the 2024 election to track deepfake disinformation campaigns and support counterintelligence efforts.[27]

1.5 — Diversify and Strengthen the Federal Cyberspace Workforce: Congress remains focused on cyber workforce issues, introducing multiple pieces of legislation to grow the federal workforce and establish a centralized training hub for early- to mid-career federal cybersecurity personnel.[28] However, budget and staffing cuts across CISA, the State Department's Bureau of Cyberspace and Digital Policy, and the Defense Department risks undercutting the very workforce these efforts aim to build.[29]

1.5.1 — Improve Cyber-Oriented Education: For the past three years, CISA has taken the leading role in K-12 cybersecurity education through its Cyber Defense and Education Training program.[30] However, in FY26, the Trump administration proposed cutting $45.4 million from the program's $206.7 million budget,[31] undermining CISA's ability to support cybersecurity awareness, training, and education programs for K-12 teachers across the country.

Pillar 2: Strengthen Norms and Non-Military Tools

Strengthen Norms and Non-military Tools						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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: The Bureau of Cyberspace and Digital Policy (CDP) was established in April 2022 and codified through the Cyber Diplomacy Act in the FY23 NDAA.[32] Following the departure of the inaugural ambassador-at-large, Nathaniel Fick, on January 20, 2025,[33] the position remains vacant, with no nominee put forth by the Trump administration. Funding and staffing cuts are jeopardizing the department's ability to sustain cyber diplomacy efforts,[34] downgrading this recommendation from full to partial implementation.

2.1.1 — Strengthen Norms of Responsible State Behavior in Cyberspace: In April 2025, Secretary of State Marco Rubio proposed a department-wide reorganization that would downgrade the CDP from a bureau-level entity.[35] This move contradicts then-Sen. Rubio's 2020 assertion that "democratic allies are integral to our way of life"[36] and runs counter to the intent of the Cyber Diplomacy Act of 2021, which elevated CDP to lead international cyber diplomacy. Despite the proposed reorganization, CDP continued to represent U.S. interests in key multilateral forums, including the United Nations Open-Ended Working Group. The working group, which adopted a consensus report in July 2025, concluded its mandate and established a new Global Mechanism to advance responsible state behavior in cyberspace.[37]

2.1.2 — Engage Actively and Effectively in Forums Setting International ICT Standards: Effective U.S. participation in international standards-setting bodies is critical to promoting secure and interoperable technology frameworks. Agencies like the National Institute of Standards and Technology, CDP, and CISA play a central role in shaping global norms. However, recent budget cuts to these agencies[38] — along with Trump's vow to dismantle the CHIPS and Science Act[39] — risk undermining U.S. leadership in key international standards forums. A proposed U.S. withdrawal from the World Trade Organization's key Information Technology Agreement commitments[40] further signals that Washington is backsliding in standards-setting efforts.

2.1.3 — Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance: On January 24, 2025, Secretary of State Marco Rubio ordered a 90-day pause on the State Department's foreign aid to assess program effectiveness.[41] Following the review, on March 10, he announced the cancellation of 83 percent of U.S. Agency for International Development foreign aid contracts — over $60 billion in total — including more than $175 million in cyber-related assistance.[42] The cuts eliminated more than a dozen programs supporting allies and partners in building cyber capacity,

including efforts to block Huawei deployment and a $95 million contract that helped train cybersecurity personnel across Eastern Europe.[43] While some aid remained through CDP-administered programs, the rollback undercuts high-impact efforts that support U.S. strategic interests in securing digital infrastructure and strengthening allies and partners.

2.1.4 — Improve International Tools for Law Enforcement Activities in Cyberspace: The FBI has expanded its international cyber presence, including opening a new law enforcement attaché office in Wellington, New Zealand — a Five Eyes partner — to counter Chinese malign activity and cybercrime.[44] It is also continuing to grow its network of cyber-focused assistant legal attachés, with upward of 22 now stationed in key embassies to strengthen coordination with allies. However, the proposed 5 percent budget cut and reduction of 1,830 personnel across the bureau could undermine the FBI's ability to respond to cyber threats and coordinate across field office operations.[45]

> ***"[The FBI] is also continuing to grow its network of cyber-focused assistant legal attachés, with upward of 22 now stationed in key embassies to strengthen coordination with allies. However, the proposed 5 percent budget cut and reduction of 1,830 personnel across the bureau could undermine the FBI's ability to respond to cyber threats and coordinate across field office operations."***

2.1.5 — Leverage Sanctions and Trade Enforcement Actions: No legislative action has been taken since last year to codify Executive Order 13848, which responds to foreign interference in the United States by employing sanctions. However, on September 9, 2024, President Joe Biden extended the authorities under the executive order to September 2025, the third extension since it was originally set to expire in 2022.[46] In January 2025, the Treasury Department's Office of Foreign Assets Control sanctioned a Chinese hacker and his company for targeting U.S. Treasury systems and telecom infrastructure in the Salt Typhoon campaign.[47]

2.1.6 — Improve Attribution Analysis and the Attribution-Decision Rubric: Over the past five years, the U.S. government has more rapidly and more regularly attributed malicious cyber operations to specific state-backed groups. In July 2025, the NSA's Cybersecurity Collaboration Center Director Kristina Walter asserted that the FBI and private sector detection, attribution, and mitigation capabilities have prevented Chinese hackers from maintaining long-term footholds in specific U.S. critical infrastructure networks.[48] However, executive action is needed to standardize attribution analysis and decision rubric.

2.1.7 — Reinvigorate Efforts To Develop Cyber Confidence-Building Measures: On July 11, 2025, the United Nations Open-Ended Working Group concluded with a consensus report endorsing eight voluntary global cyber confidence-building measures and launching a new Global Mechanism to advance responsible state behavior.[49] Recent cuts to the State Department's diplomatic cyber programs[50] may limit the United States' ability to operationalize these measures to build cyber confidence-building measures.

Pillar 3: Promote National Resilience

Promote National Resilience						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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: Congress codified sector risk management agencies in law through the FY21 NDAA,[51] and an April 2024 presidential memorandum reaffirmed their roles.[52]

3.1.1 — Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy: The April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience fully implemented this recommendation by directing the DHS, through CISA, to create a coordinated national risk management cycle and develop sector-specific risk assessments and risk management plans that will be integrated into a biennial National Infrastructure Risk Management Plan.[53]

3.1.2 — Establish a National Cybersecurity Assistance Fund: On August 1, 2025, CISA and the Federal Emergency Management Agency announced a funding opportunity worth more than $100 million for state, local, and tribal cybersecurity programs.[54] While these programs align with the intent of this recommendation, the delayed rollout and limitations to how grant recipients can use the funds underscore the need for a dedicated National Cybersecurity Assistance Fund to ensure timely, flexible, and long-term support.

3.2 — Develop and Maintain Continuity of the Economy Planning: In 2023, the Biden administration submitted its Continuity of the Economy plan to Congress as mandated by the FY21 NDAA,[55] but it largely dismissed congressional concerns of inadequate existing government incident response and emergency management planning. The Trump administration has repeatedly signaled its prioritization of economic resilience and should revisit Continuity of the Economy planning, integrating industry input and clarifying federal roles.[56]

3.3 — Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund": Provisions in the Infrastructure Investment and Jobs Act of 2021 implemented this recommendation.[57]

3.3.1 — Designate Responsibilities for Cybersecurity Services Under the Defense Production Act: While the DOD can utilize the Defense Production Act (DPA) to accelerate the procurement of critical cybersecurity technologies and allow modifications to acquisition requirements, the department has not formally designated cybersecurity services under the DPA. The reauthorization of the DPA (set to expire in September 2025)[58] presents an opportunity to include cybersecurity services as a national security priority within its framework.

3.3.2 — Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts: Congress has not taken any legislative action over the past year to protect companies acting under federal or law enforcement direction during cyber and emergency response efforts.

3.3.3 — Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts: In December, CISA released a draft of the National Cyber Incident Response Plan for comment.[59] The draft, however, did not provide clarity on the roles and responsibilities of federal, state, local, tribal, and territorial governments and private entities when responding to significant cyber incidents affecting critical infrastructure. It is unclear if CISA will reissue an updated draft in response to comments or if the Trump administration is starting the drafting process over.

3.3.4 — Expand Coordinated Cyber Exercises, Gaming, and Simulation: The FY22 NDAA implemented this recommendation.[60] However, both the Biden and Trump administrations proposed budgetary cuts to the National Infrastructure Simulation Analysis Center,[61] eroding the federal government's capacity to conduct national cyber exercises.

3.3.5 — Establish a Biennial National Cyber Tabletop Exercise: The FY21 NDAA implemented this recommendation, ensuring regular cyber preparedness drills for critical infrastructure.[62]

3.3.6 — Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard: The National Guard continues to expand its role in international cyber capacity building, participating in national and international exercises and working with allies to strengthen collective cyber defense.[63]

3.4 — Improve the Structure and Enhance Funding of the Election Assistance Commission: Between 2020 and 2023, states spent more than $638 million from Help America Vote Act election security and cybersecurity grants.[64] Despite this demonstrated need, federal investment remains inconsistent. The president's FY26 budget request included no funding for election security grants. The House version of the annual appropriations bill provides only $15 million for these grants and reduces the Election Assistance Commission's base funding.[65] Meanwhile, the Election Security Information Sharing Analysis Center shut down after the Trump administration eliminated CISA's funding for the effort.[66]

3.4.1 — Modernize Campaign Regulations to Promote Cybersecurity: On September 19, 2024, the Federal Election Commission finalized a rule allowing federal candidates, officeholders, their families, and staff to use campaign funds for cybersecurity and physical measures.[67] This marks meaningful progress, but Congress has not amended 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 May 9, 2025, Trump terminated the $2.75 billion Digital Equity Act programs — created under the bipartisan Infrastructure Investment and Jobs Act of 2021 — which provided states and local governments grants to expand access to digital literacy education, citing "race-based" criteria as unconstitutional.[68] However, private companies and local governments continue to invest in digital literacy programs, which help build societal resilience against foreign malign influence.[69]

3.5.1 — Reform Online Political Advertising to Defend Against Foreign Influence in Elections: In October 2024, the ODNI Office of the Director of National Intelligence warned that China, Iran, and Russia are "better prepared" to influence future general elections based on lessons learned from the 2020 election.[70] Despite this assessment, there has been no meaningful federal action to limit foreign government funding in online political advertising, and the Trump administration has shuttered efforts at the FBI, CISA, and the State Department to identify and combat foreign malign influence.[71]

Pillar 4: Reshape the Cyber Ecosystem Toward Greater Security

Reshape the Cyber Ecosystem Toward Greater Security						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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: In January 2025, after 18 months of public input, the Federal Communications Commission (FCC) formally launched the U.S. Cyber Trust Mark, a cybersecurity certification and labeling program for consumer smart devices.[72] The initiative was initially welcomed by industry stakeholders. However, in June 2025, FCC Chairman Brendan Carr paused the program and launched an investigation into UL Solutions — the FCC-authorized testing and certification body that administers the program — over its joint venture with China National Import and Export Commodities Inspection Corp.,[73] raising concerns about the program's long-term viability and credibility.

4.1.1 — Create or Designate Critical Technology Security Centers: This recommendation was partially implemented through appropriations from the Infrastructure Investment and Jobs Act to the DHS's Science and Technology Directorate.[74]

4.1.2 — Expand and Support the National Institute of Standards and Technology Security Work: At the direction of the Office of Management and Budget, the National Institute of Standards and Technology (NIST) fired 20 percent of its workforce — about 500 employees — including those hired under the CHIPS and Science Act.[75] Additionally, the president's FY26 budget sought to eliminate an additional 650 positions[76] and cut $325 million in NIST funding.[77] House and Senate appropriators, however, rejected the proposed budget cuts, increasing NIST's funding instead.[78] Sustained appropriations are needed to meet NIST's expanded responsibilities and maintain the United States' competitive edge in critical technologies such as AI, quantum computing, and advanced manufacturing.

4.2 — Establish Liability for Final Goods Assemblers: In January 2025, outgoing National Cyber Director Coker said the ONCD developed policy considerations for the incoming administration and Congress on liability for software vulnerabilities.[79] In the final days of his administration, Biden issued an executive order requiring federal contractors to submit secure software attestations, validation artifacts, and federal customer lists to CISA for review.[80] On June 6, 2025, however, Trump issued another executive order removing these attestation and validation provisions but retaining requirements that NIST update the secure software development framework and related guidance on secure software delivery.[81]

4.2.1 — Incentivize Timely Patch Implementation: As noted last year, NIST's National Vulnerability Database continues to face budget shortfalls and capacity constraints. As of August 2025, the database has a backlog of nearly 15,000 vulnerabilities,[82] leaving organizations without timely information to guide patching for security flaws. The related Common Vulnerabilities and Exposures program, which assigns standardized identifiers for newly disclosed vulnerabilities, also nearly went dark when the federal contract for the program came within 24 hours of expiring.[83] Without sustained appropriations for these programs, the United States risks losing its position as the global leader on vulnerability management and undermining the ability of organizations to implement timely patches.

4.3 — Establish a Bureau of Cyber Statistics: Congress has not yet created a Bureau of Cyber Statistics. Trump's removal of senior statistical leadership and periods of temporary loss of public access to government data[84] have introduced governance risk to the integrity of official statistics,[85] creating a climate where movement on this recommendation is unlikely.

4.4 — Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications: While adoption of state-level data security standards for insurers and licensees is increasing each year,[86] implementation varies by state, and there are no national baselines for underwriting and claims practices. Industry stakeholders continue to call for greater clarity and standardization in cyber policy terms to expand coverage availability and reduce uncertainty for insured and insurers alike.[87]

4.4.1 — Establish a Public-Private Partnership on Modeling Cyber Risk: In its March 2025 letter to Congress, the National Association of Insurance Commissioners — a standard-setting body for state insurance regulators — expressed support for improving cyber risk modeling but opposed federal preemption, arguing that any modeling initiative must respect each state's jurisdiction.[88] However, this fragmented state-by-state approach risks leaving systemic gaps in national preparedness. A month prior, NIST released a report arguing that pooling and organizing data across sectors — and mapping dependencies and modeling systemic scenarios — are essential for accurately pricing and mitigating cyber risk.[89] A DHS-led public-private working group remains essential to developing models that both inform the cyber insurance market and strengthen overall resilience.

4.4.2 — Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events: Since last year's call for proposals for terrorism and cyber risk research,[90] the Treasury's Federal Insurance Office and the National Science Foundation have provided researchers at higher education institutions with grant funding to advance research in this area.[91] Other research institutions have also published reports on the need for a federal backstop.[92] Continued federal action is needed to evaluate reinsurance options that can mitigate catastrophic cyber events and provide market stability.

4.4.3 — Incentivize Information Technology Security Through Federal Acquisition Regulations and Federal Information Security Management Act Authorities: While the Biden administration implemented this recommendation through a May 2021 executive order, in April, Trump issued an executive order directing federal agencies to rewrite the Federal Acquisition Regulation to prioritize low-cost commercial technologies while eliminating non-statutory provisions, including cybersecurity guardrails.[93] While the rewrite could benefit the federal government with faster delivery of services, without careful consideration for cyber and supply chain security provisions, it could expand national security risks.

4.4.4 — Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements: The Security and Exchange Commission's rules, requiring publicly traded companies to disclose material cybersecurity incidents and update cybersecurity risk management policies annually, implemented this recommendation.[94]

4.5 — Develop a Cloud Security Certification: In July 2024, the Office of Management and Budget issued a memorandum directing the General Services Administration (GSA) to "accelerate the adoption of cloud computing products."[95] At the time of the issuance, Federal Risk and Authorization Management Program authorizations were projected to take more than a year.[96] In March 2025, the GSA launched a pilot to streamline the authorization process built around industry input and the use of automation.[97] Five months later, in August 2025, the GSA announced that the FedRAMP services approvals increased from 49 authorizations in FY24 to 114 authorizations in FY25.[98]

4.5.1 — Incentivize the Uptake of Secure Cloud Services for Small- and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments: The State and Local Cybersecurity Improvement Act, passed into law in the bipartisan Infrastructure Investment and Jobs Act, partially implemented this recommendation.[99]

4.5.2 — Develop a Strategy to Secure Foundational Internet Protocols and Email: 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. There have been continued federal efforts in BGP and DNS security. In September 2024, the ONCD released its Roadmap to Enhancing Internet Routing Security, calling for widespread adoption of Resource Public Key Infrastructure, which verifies the authenticity of internet routing information, making it more difficult for hackers to hijack internet traffic.[100] In July 2025, CISA issued an interagency joint advisory highlighting protective DNS as one of the effective defenses against Interlock ransomware actors targeting critical infrastructure across North America and Europe.[101] The advisory emphasized the effectiveness of early interception of malicious traffic before a connection is established. These actions align with NIST's initial public draft of "Border Gateway Protocol Security and Resilience," published in January 2025, calling for widespread adoption of Resource Public Key Infrastructure to mitigate BGP vulnerabilities.[102] In May 2025, CISA updated its December 2024 guidance, expanding requirements for federal civilian agencies to strengthen cloud security baselines and remediate configuration vulnerabilities.[103]

"[I]n April, Trump issued an executive order directing federal agencies to rewrite the Federal Acquisition Regulation to prioritize low-cost commercial technologies while eliminating non-statutory provisions, including cybersecurity guardrails. While the rewrite could benefit the federal government with faster delivery of services, without careful consideration for cyber and supply chain security provisions, it could expand national security risks."

4.5.3 — Strengthen the U.S. Government's Ability to Take Down Botnets: Over the past year, U.S. law enforcement agencies expanded joint operations to disrupt major Chinese and Russian-linked botnets through sanctions, indictments, and victim notification orders. On September 28, 2024, in coordination with allied partners, they exposed and issued public mitigation guidance on a People's Republic of China-linked botnet controlling over 260,000 devices responsible for more than 1.2 million compromised devices worldwide, including 385,000 in the United States.[104] On January 3, 2025, the Treasury Department sanctioned related Integrity Technology Group, a cybersecurity company linked to the Chinese Ministry of State Security.[105] On May 9, 2025, the Department of Justice (DOJ) announced the dismantlement and indictment of separate groups of Russian and Kazakhstani hackers for deploying malware to build and monetize networks of compromised devices, followed by a July 23, 2025, victim assistance order directing the federal government to issue notices to these victims.[106]

4.6 — Develop and Implement an ICT Industrial Base Strategy: Previously, the CHIPS and Science Act[107] and other executive actions[108] had partially implemented this recommendation and continued to advance this recommendation. On August 1, 2025, the International Trade Administration highlighted Germany as a key market for U.S. ICT exports and investment,[109] while in May 2025, the National Telecommunications and Information Administration announced that 35 projects received $550 million in awards to support ICT research and development and commercialization through the CHIPS and Science Act.[110]

4.6.1 — Increase Support to Supply Chain Risk Management Efforts: The February 2021 executive order on supply chain resiliency and the passage of the CHIPS and Science Act fully implemented this recommendation.[111] On June 4, 2025, NIST released the public draft of SP 800-18's second revision, "Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems," providing updated guidance to align with the NIST Risk Management Framework, Privacy Framework, and cybersecurity supply chain risk management practices. The public comment period closed on July 30, 2025.[112]

4.6.2 — Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies: Over the past five years, Congress has consistently funded emerging technologies research and development,[113] with the CHIPS and Science Act securing long-term investment.[114] However, within 50 days of taking office,[115] the Trump administration crippled America's scientific backbone, freezing $2.2 billion in research funds that had sustained universities and laboratories across the country[116] — eroding U.S. competitiveness at the exact moment global rivals have begun to accelerate their own research and development programs.[117]

4.6.3 — Strengthen the Capacity of the Committee on Foreign Investment in the United States: A September 2022 executive order expanded the factors the Committee on Foreign Investment in the United States (CFIUS) uses during its review process.[118] In November 2024, the Treasury Department issued a rule adding over 60 military installations to CFIUS's real estate jurisdiction and expanding coverage around 10 existing installations.[119] On August 6, 2025, CFIUS published its annual report for Congress, which showed a higher volume of covered transactions in 2024 than in the prior year.[120]

4.6.4 — Invest in the National Cyber Moonshot Initiative: On January 20, 2025, the Trump administration suspended all advisory committees reporting to the DHS, including the National Security Telecommunications Advisory Committee — effectively dismantling a key advisory body for the Cyber Moonshot Initiative.[121]

4.7 — Pass a National Data Security and Privacy Protection Law: In February 2025, House Republicans created a privacy working group to develop a national data privacy standard framework.[122] Separately, in April, the DOJ implemented a data security program to prevent foreign adversaries from accessing Americans' sensitive personal data.[123]

4.7.1 — Pass a National Breach Notification Law: While various federal and state regulations require companies to notify consumers of data breaches under certain circumstances, there is no comprehensive federal requirement.

Pillar 5: Operationalize Cybersecurity Collaboration With the Private Sector

Operationalize Cybersecurity Collaboration With the Private Sector						
Rec. Number	Recommendations Title	2021	2022	2023	2024	2025
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": An April 2024 presidential national security memorandum tasked CISA with working with the other sector risk management agencies to identify systemically important entities within each critical infrastructure sector that have a disproportionate impact on U.S. national security, economic security, and public health and safety.[124] There have been no public updates since that time, but workforce reductions at CISA may be impeding the development of a systemically important entities list. The Trump administration is also reportedly considering revisions to the April 2024 memorandum.

5.1.1 — Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector: Under the reduction in force, CISA lost nearly a third of its workforce, including personnel who facilitated information exchange, a reduction that many have said has "severely affected" the agency's ability to engage meaningfully with industry stakeholders.[125] There have been mixed reviews on the government's effectiveness in sharing timely, actionable threat intelligence with the private sector. In the wake of the Salt Typhoon breach, major telecommunications providers learned of the compromise from the media before being alerted by federal agencies.[126] In July 2025, the Government Accountability Office reported that the Cybersecurity Information Sharing Act of 2015 "positively contributed" to information sharing between federal and nonfederal entities, enabling data sharing tools and implementing guidelines on how entities exchange and receive critical information.[127] Before the bill was set to expire on September 30, 2025, CISA leaders were "really hopeful" for its reauthorization and stressed that the "rapid sharing" of information is vital to protecting U.S. critical infrastructure from persistent cyber threats.[128] However, the bill ultimately expired amid the October 2025 government shutdown, with a CISA spokesperson calling the lapse "a serious blow" to the U.S. government's cybersecurity posture.[129]

5.1.2 — Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities: Many large technology firms and cybersecurity providers continue to express confidence in the integrity of information-sharing channels with the federal government.[130] Federal agencies are also maintaining interagency efforts to

ensure the private sector has access to timely, relevant cyber threat intelligence.[131] Strengthening statutory privacy and liability protections, along with consistent classification of information, remains important to rebuilding trust and enabling more effective public-private intelligence information sharing.

5.1.3 — Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities: The FY21 NDAA implemented this recommendation by providing CISA with administrative subpoena authority.[132] Using this authority, CISA contacted more than 3,000 entities to help them remove vulnerable industrial control system devices from the internet.[133]

5.2 — Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information: The Salt Typhoon breach exposed major breakdowns in how threat information is exchanged between the government and industry.[134] A Joint Collaborative Environment (JCE) remains necessary as a real-time threat intelligence hub to ensure critical cyber threat data is shared quickly and reliably. The FY26 president's budget request, however, proposes to cut $36.5 million from JCE efforts at CISA.[135] House appropriators instead directed CISA to provide semiannual briefings on the plan, timeline, and funding necessary to transition from the existing mechanism to the JCE.[136]

5.2.1 — Expand and Standardize Voluntary Threat Detection Programs: The FY22 NDAA codified CyberSentry, a voluntary program through CISA that provides continuous monitoring and detection of cybersecurity threats on critical infrastructure networks.[137] Press reporting indicates, however, that contract lapses have hamstrung the ability of national labs to analyze data and provide information back to participants.[138] The program requires stable, multiyear funding and contractual continuity to avoid operational gaps.

5.2.2 — Pass a National Cyber Incident Reporting Law: The passage of the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 fully implemented this recommendation,[139] and CISA has been receiving industry feedback to develop the final regulations.[140] Outgoing CISA Director Jen Easterly warned in January that conflicting timelines and definitions between this law and existing cyber incident reporting rules could create a "recipe for dysfunction."[141] Lawmakers have also criticized drafts of the proposed rule for being overly broad and burdensome.[142] Timely issuance of the final rule by the October statutory deadline will be critical to ensuring clarity and trust between government and industry.[143]

5.2.3 — Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors: The commission proposed an amendment to the Pen Register Trap and Trace Devices Statute with the intent of allowing companies with the necessary resources and expertise to conduct defensive activities on behalf of themselves or their customers. Congress has not yet acted on this proposal.

5.3 — Strengthen an Integrated Cyber Center Within CISA and Promote the Integration of Federal Cyber Centers: Over the past year, CISA issued various joint cybersecurity advisories and products with interagency and international partners — issuing 58 in 2024[144] — collaborating with federal agencies across the government, including the NSA, FBI, the ODNI, the DOJ, and the DOD. [145] While these joint outputs reflect progress toward coordinated analysis and response to significant cybersecurity incidents, persistent gaps in real-time information exchange with other public and private entities can and do hinder the government's ability to present a unified operational picture to industry partners.

5.4 — Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency: The FY21 NDAA fully implemented this recommendation.[146] Now known as CISA's Joint Cyber Defense Collaborative (JCDC), it has over 300 participating organizations.[147] Earlier this year, however, JCDC saw a significant workforce reduction. Without sufficient personnel, plans to onboard hundreds of additional partners have stalled.[148] Without resources and expertise, JCDC cannot coordinate joint cyber defense activities with industry and government partners.[149]

5.4.1 — Institutionalize DOD Participation in Public-Private Cybersecurity Initiatives: The FY22 NDAA implemented this recommendation,[150] and the Defense Department continues to demonstrate its commitment to improving public-private partnerships, highlighting their value as a force multiplier for military readiness.[151]

5.4.2 — Expand Cyber Defense Collaboration With ICT Enablers: The FY22 NDAA created voluntary and pilot programs that implemented this recommendation.[152]

Pillar 6: Preserve and Employ Military Instruments of Power

Preserve and Employ Military Instruments of Power						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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 Defense Industrial Base 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: The FY21 NDAA implemented this recommendation by mandating a force structure assessment. The FY25 NDAA further advanced this effort by directing an independent study of how to improve cyber force generation in the U.S. military, including the possibility of creating a separate cyber service.[153] Parallel with government efforts, in August, the Center for Strategic and International Studies and CSC 2.0 announced a new commission to examine the practical requirements of standing up a dedicated Cyber Force.[154]

6.1.1 — Direct DOD to Create a Major Force Program Funding Category for U.S. Cyber Command: The FY21 and FY22 NDAAs implemented this recommendation, providing U.S. Cyber Command with enhanced budgetary authority. Last year, Congress appropriated $1.6 billion for the U.S. Cyber Command.[155]

6.1.2 — Expand Current Malware Inoculation Initiatives: U.S. Cyber Command, in particular, continues to share malware and other threat information with private partners through its Under Advisement program.[156] In FY26, the U.S. Cyber Command requested a $117.2 million increase for its Data and Sensors research and development portfolio, a substantial increase from the $21 million requested in the FY25 budget. Prior investments have already contributed to a 52 percent decrease in "anomalous behavior" and a 32 percent drop in vulnerabilities across Guam's networks.[157]

6.1.3 Review Delegation of Authorities for Cyber Operations: The FY21 NDAA implemented this recommendation by delegating cyber-related authorities to the commander of U.S. Cyber Command.[158]

6.1.4 — Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces: 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.[159] Since the revelation of the extent of Chinese penetration of U.S. critical

infrastructure, lawmakers have argued for a need to "revamp" the rules of engagement and increase the speed and unity of effort in cyber operations.[160] The House and Senate versions of the FY26 NDAA contain provisions to study cyber force employment and the creation of Joint Task Force-Cyber to streamline command and control across geographic combatant commands.[161]

6.1.5 — Cooperate With Allies and Partners to Defend Forward: In the 2025 posture statement, then-acting U.S. Cyber Command Cmdr. Lt. Gen. William Hartman reported that in 2024, the Cyber National Mission Force deployed more than 85 times to over 30 partner nations, across all geographic commands.[162]

6.1.6 — Require DOD to Define Reporting Metrics: 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.[163] In July 2025, the Government Accountability Office reported that the DOD has implemented mechanisms to strengthen its interoperability with foreign partners, but more work is needed to close personnel gaps and sustain partner integration.[164]

6.1.7 — Assess the Establishment of a Military Cyber Reserve: The FY24 NDAA authorized the secretary of the Army to conduct a pilot program on creating a civilian cybersecurity reserve.[165] The Senate version of the FY26 NDAA includes a provision requiring the Defense Department to report on and develop an implementation plan to integrate reserve components — particularly the National Guard under Title 32 authorities — into cyber mission forces.[166] This progress reflects growing congressional interest in leveraging reserve cyber talent to bolster national cyber readiness.

6.1.8 — Establish Title 10 Professors in Cyber Security and Information Operations: The FY24 NDAA directed the DOD to establish the Cyber Academic Engagement Office to foster relationships with academic institutions, manage cyber-related educational programs, and oversee the development of cyber skills within the U.S. military.[167] In August 2024, Diba Hadi became the new principal director for the Cyber Academic Engagement Office.[168] Under her leadership, the office is streamlining collaboration and communication with academia, industry, and government partners.[169]

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: Legislation and executive actions have mandated comprehensive reviews, evaluations, and the development of secure nuclear command, control, and communications systems.[170] The FY24 NDAA in particular established a DOD working group to inventory and mitigate risks, ensuring continuous assessment and improvement.[171]

6.2.1 — Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program: Two initiatives implemented this recommendation last year. In April 2024, the Defense Industrial Base Cybersecurity Program expanded to grant 68,000 additional contractors access to technical exchange meetings, a collaborative web platform, and threat information products and services through the DOD's Cyber Crime Center.[172] Additionally, the center and the Defense Counterintelligence and Security Agency launched a strategic partnership establishing a vulnerability disclosure program for the defense industrial base.[173] Just six months after its launch, the DOD estimates that the program has "saved contractors hundreds of millions of dollars" in response and recovery costs.[174] In November 2024, the NSA's Cybersecurity Collaboration Center also launched an AI-powered autonomous penetration testing platform that continuously simulates adversarial actions to analyze attack behavior and identify vulnerabilities across networks.[175]

6.2.2 — Require Threat Hunting on Defense Industrial Base Networks: The FY21 NDAA[176] partially addressed this recommendation by mandating an assessment of the feasibility of implementing a defense industrial base cybersecurity threat-hunting program. In October 2024, the DOD released the final rule for the Cybersecurity Maturity Model Certification 2.0 program.[177] While the program strengthens baseline security across the defense industrial base, this recommendation is not yet fully implemented.

6.2.3 — Designate a Threat-Hunting Capability Across the DOD Information Network: The FY22 NDAA implemented this recommendation by requiring threat hunting and discovery of malicious activity across the Defense Department's information network.[178]

6.2.4 — Assess and Address the Risk to National Security Systems Posed by Quantum Computing: The FY21 NDAA implemented this recommendation by requiring an assessment of the potential threats and risks posed by quantum computing.[179] Building on this, the FY24 NDAA included a pilot program for quantum computing applications to address technical challenges and enhance capabilities.[180] The FY25 NDAA included various provisions for the Pentagon to develop and advance its quantum strategy.[181]

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	2025
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: The State and Local Cybersecurity Improvement Act, passed as part of the Infrastructure Investment and Jobs Act, implemented this recommendation.[182] As of August 2024, $172 million has been invested across 33 states and territories to fund 839 state and local cybersecurity projects.[183] Disconcertingly, however, the most recent notice of funding opportunity prohibits states from using funds to purchase services from the Multi-State Information Sharing and Analysis Center.[184] It has been a critical cybersecurity service provider to state and local governments and municipally owned utilities.

Pandemic 1.2 — Pass an Internet of Things Security Law: In January 2025, the FCC launched the U.S. Cyber Trust Mark program to certify secure consumer Internet of Things (IoT) devices,[185] but in June 2025 the program was paused pending an investigation into its authorized testing body.[186] This development underscores the need for congressional action to codify an IoT law with strong oversight mechanisms.

Pandemic 1.3 — Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts: In the 2024 general election cycle, Election Infrastructure Information Sharing Analysis Center (EI-ISAC), a nonprofit housed at the Center for Internet Security, worked closely with law enforcement, election officials, and other state and local partners to provide cybersecurity services. Preparation began in 2022, and on Election Day 2024, the Center for Internet Security and EI-ISAC blocked 50 cyberattacks, prevented 138,782 connections to malicious domains, and countered text message-based disinformation campaigns and bomb threats while operating a virtual situation room with 1,300 participants.[187] However, recent federal funding cuts to CISA have eliminated EI-ISAC's primary funding stream, forcing the organization to seek alternative funding to continue its services.[188] Sustained federal investment is essential for nonprofits working with law enforcement to continue providing these capabilities.

Pandemic 1.4 — Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns: While the DOJ and the National Science Foundation have previously provided grant funding for research on foreign malign influence,[189] Trump's executive order on "Restoring Freedom of Speech and Ending Federal Censorship" halted all federal grant programs supporting this work — including those at other federal agencies.[190] This move has significantly reduced funding for nongovernmental efforts to expose foreign malign influence campaigns targeting the American public. Meanwhile, the administration cut all funding for EI-ISAC, which had worked closely with law enforcement, election officials,

and other state and local partners to provide cybersecurity services, counter physical and cyber threats, and identify foreign malign influence campaigns against U.S. elections.[191]

Pandemic 1.4.1 — Establish the Social Media Data and Threat Analysis Center: The FY23 NDAA tasked the director of national intelligence with submitting "a plan to operationalize" the Social Media and Threat Analysis Center,[192] but the director has not yet submitted the plan to Congress.

White Paper #2: National Cyber Director

National Cyber Director					
Rec. Number	2021	2022	2023	2024	2025
NCD 1					

Establish a National Cyber Director: The FY21 NDAA created the ONCD.[193] In January, outgoing Director Coker noted that ONCD still relies more on informal authority than statutory power, lacking an independent convening role, a budgetary directive authority, or a mandate to harmonize federal cyber regulations.[194] In August 2025, the U.S. Senate confirmed Cairncross as the third national cyber director.[195] While ONCD is now institutionalized and resourced with an 85-person staff,[196] further congressional action could strengthen its authorities and sustain long-term impact.

White Paper #3: Growing a Stronger Federal Cyber Workforce

Growing a Stronger Federal Cyber Workforce						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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: 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.[197] As the new national cyber director takes the helm at ONCD, maintaining cyber workforce leadership and coordination structures will be important to developing the workforce necessary to address today and tomorrow's cyber and technology challenges.

Workforce 2 — Properly Identify and Utilize Cyber-Specific Occupational Classifications: The Office of Personnel Management reaffirmed efforts to improve STEM recruiting and streamline hiring under its May 2025 Merit Hiring Plan.[198] While reforms to modernize cyber-specific classifications continue, the revival of Schedule F and at-will employment complicate progress toward a purely competency-based cyber workforce.

Workforce 3 — Develop Apprenticeships: The federal government continues to implement this recommendation. At the end of June, the Department of Labor awarded another $84 million in grants for state apprenticeship programs, noting that this funding will grow registered apprenticeship programs in technology, artificial intelligence, and advanced manufacturing.[199]

"In August 2025, the U.S. Senate confirmed Cairncross as the third national cyber director. While ONCD is now institutionalized and resourced with an 85-person staff, further congressional action could strengthen its authorities and sustain long-term impact."

Workforce 4 — Improve Cybersecurity for K-12 Schools: Earlier this year, the Department of Education disbanded the Office of Educational Technology,[200] which provided cybersecurity guidance for schools, and the Education Government Coordinating Council, an interagency effort that collaborated with 13 nonprofit organizations to coordinate cyber defense for the sector.[201] At the same time, cuts to CISA's funding for the Multi-State Information Sharing and Analysis Center jeopardize the free incident response, threat sharing, and cybersecurity training services that many school districts rely on.[202] In July, more than 400 school district officials petitioned for the reinstatement of the center and other K-12 cybersecurity funding as well as the reinstatement of the Office of Educational Technology.[203]

Workforce 5 — Provide Work-Based Learning via Volunteer Clinics: In 2023, the NSA established cyber clinics in four states to support communities and local governments with cyber risk assessment and planning assistance,[204] fully implementing this recommendation. Private sector companies and university-based cyber clinics are also conducting similar efforts.[205]

Workforce 6 — Improve Pay Flexibility and Hiring Authorities: In September 2024, the Office of Personnel Management extended federal agencies' direct hiring authorities for STEM and cybersecurity and related positions through the end of 2028.[206] However, under the Trump administration, progress toward modernizing federal cyber hiring has been uneven: a government-wide hiring freeze[207] and workforce cuts have constrained agencies' ability to use these authorities.[208] The Trump administration's reduction in force disproportionately affected early-career probationary staff,[209] including those recruited through new cyber talent pipelines.[210]

Workforce 7 — Incentivize Cyber Workforce Research: The passage of the CHIPS and Science Act fully implemented this recommendation.[211] However, the Trump administration's elimination of diversity, equity, and inclusion programs — including CISA's pilot program to hire neurodiverse individuals — has curtailed critical data collection on workforce needs and outcomes.[212]

Workforce 8 — Mitigate Retention Barriers and Invest in Diversity in Recruiting: The Biden administration made progress in efforts to retain qualified personnel and recruit from nontraditional communities.[213] However, the Trump administration's sweeping rollback of diversity, equity, and inclusion programs[214] has sharply reversed momentum, with the potential to exacerbate cyber workforce shortages.[215] While then-House Homeland Security Committee Chairman Rep. Mark Green (R-TN) introduced legislation in February to improve opportunities for community college and technical school graduates,[216] the political environment surrounding workforce cuts has damaged what had been bipartisan support for efforts to develop the federal cyber workforce.[217]

White Paper #4: Building a Trusted ICT Supply Chain

Building a Trusted ICT Supply Chain						
Rec. Number	Recommendation Title	2021	2022	2023	2024	2025
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: Executive Order 14017, "America's Supply Chains," fully implemented this recommendation.[218] There have been various initiatives continuing across the federal government to advance this effort.[219]

Supply Chain 2 — Identify Key ICTs and Materials: The DHS published the "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry" in February 2022, fully implementing this recommendation.[220]

Supply Chain 3 — Conduct a Study on the Viability of Critical Technology Clusters and Designate Them: 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.[221] In January 2025, the Biden administration awarded $504 million in grants to 12 Tech Hubs, but under the new Trump administration, Commerce Secretary Howard Lutnick rescinded six of those awards. In May 2025, the program was revised and relaunched with a $220 million loan instead of a grant, available for new recipients.[222]

Supply Chain 3.1 — Provide Research and Development Funding for Critical Technologies: The CHIPS and Science Act implemented this recommendation and spurred additional investments in research and development for critical technologies. For instance, in July 2025, the National Science Foundation's Regional Innovation Engines program advanced 29 semifinalists in its competition, spanning projects from critical minerals mining to advanced optical sensors, each led by public-private coalitions. Finalists, to be announced in early 2026, will receive $160 million over 10 years.[223]

Supply Chain 3.2 — Incentivize the Movement of Critical Chip and Technology Manufacturing Out of China: The CHIPS and Science Act provided more than $50 billion to boost the U.S. domestic chip industry, leading to over $600 billion in private investments funding over 130 projects across 28 states. According to the Semiconductor Industry Association, these investments

are expected to create and support over 500,000 jobs across the country.[224] In March 2025, Taiwan Semiconductor Manufacturing Company announced that the company plans to invest $100 billion for advanced semiconductor manufacturing and research and development facilities in Arizona, boosting construction and engineering jobs in the United States.[225] The Trump administration has expressed strong support for reducing U.S. dependence on overseas chip production. Yet, its decision to acquire equity stakes and take a share of revenue from AI chip exports to China[226] introduces strategic and market contradictions — raising concerns about the alignment of such conditional export agreements with long-term supply chain resilience goals.

Supply Chain 3.3 — Conduct a Study on a National Security Investment Corporation: Although Congress has not created a stand-alone National Security Investment Corporation, the DOD's Office of Strategic Capital, in partnership with the Small Business Administration, has operationalized the commission's vision through the Small Business Investment Company Critical Technology Initiative. Under this initiative, the Small Business Administration can provide up to $175 million in loan guarantees per fund, leveraging federal backing to attract and scale private capital into companies developing critical technologies.[227] The first cohort of 18 approved funds — spanning investment stages from seed to buyout — is projected to channel over $4 billion in private investment to roughly 1,700 portfolio companies.[228]

Supply Chain 4 — Designate a Lead Agency for the ICT Supply Chain: The FY21 NDAA designated the DHS as the sector risk management agency for the information technology sector, fully implementing this recommendation.[229] National Security Memorandum 22 also reaffirms this designation.

Supply Chain 4.1 — Establish a National Supply Chain Intelligence Center: While a National Supply Chain Intelligence Center does not yet exist, a combination of efforts partially implemented this recommendation. Efforts by the National Counterintelligence and Security Center to lead the Supply Chain and Counterintelligence Risk Management Task Force[230] and the Supply Chain and Cyber Directorate to share sensitive information with the federal acquisition community align with this recommendation.[231]

Supply Chain 4.2 — Fund Critical Technology Security Centers: The Infrastructure Investment and Jobs Act partially implemented this recommendation.[232] While there has been previous congressional interest in creating critical technology security centers,[233] legislation has not yet been passed. Federal agencies have issued guidance,[234] and national laboratories and university programs[235] have provided testing and evaluating functions that align with this recommendation, but a dedicated center to test critical technology security is needed to fully implement this recommendation.

Supply Chain 5 — Incentivize Open and Interoperable Standards and Release More Mid-Band Spectrum: The FCC took multiple steps this past year to expand mid-band spectrum and strengthen supply chain security. As directed by Congress, the FCC adopted final rules in August regarding auctioning additional mid-band spectrum for 5G.[236] Additionally, in May 2025, the FCC adopted new rules to tighten its equipment authorization program, which oversees how telecommunications devices are tested and approved before entering U.S. markets.[237] These rules ban foreign-controlled test labs and certification bodies from approving devices in the FCC's program. Congress, meanwhile, sustained funding for the rip-and-replace program to remove Chinese telecommunications equipment from U.S. networks.[238] In July, the Government Accountability Office, however, issued a letter to the acting assistant secretary of Commerce warning that its recommendations to the National Telecommunications and Information Administration on improving spectrum management have not been addressed.[239]

Supply Chain 5.1 — Develop a Digital Risk Impact Assessment for International Partners for Telecom Infrastructure Projects: In October 2024, NIST awarded $15 million to establish a Standardization Center of Excellence led by the American Society for Testing and Materials International to bolster U.S. participation in international standardization for critical and emerging technologies.[240] However, Trump administration decisions to halt all development grants through the U.S. Agency for International Development have significantly narrowed U.S. tools,[241] leaving U.S. allies and partners with fewer alternatives to Chinese vendors while eroding the State Department's ability to drive standards-setting efforts.

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: Over the past year, the U.S. Trade Development Agency expanded support for energy, infrastructure, and manufacturing projects to reduce reliance on Chinese suppliers.[242] In January 2025, the Export-Import Bank launched its Supply Chain Resiliency Initiative to

provide targeted financing to reduce dependence on Chinese critical minerals and rare earth elements and boost American manufacturing.[243] However, the U.S. International Development Finance Corporation's authorization is set to expire in October 2025, and its inability to support projects in middle-income countries, like Panama, has allowed China to expand its investments in the region.[244] These U.S. financing tools remain constrained by outdated rules and limited authorities. Ensuring they can operate flexibly and at scale is essential not only for commercial competitiveness but also for national security.

Supply Chain 5.3 — Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects: While Congress and the Trump administration remain focused on limiting the ability of Chinese state-controlled companies to do business in the United States,[245] the administration has not created the necessary 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	2025
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 DHS 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 FCC 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: Over the past three years, Congress has consistently appropriated $23 million to the Department of Education for civic education.[246] Nongovernmental organizations have continued civic education initiatives.[247]

Countering Disinformation 2 — Ensure Material Support for Nongovernmental Disinformation Researchers: Under the Biden administration, the federal government provided more than 600 grants and contracts to researchers across nonprofit organizations and higher education institutions to conduct research on countering disinformation.[248] The Trump administration reversed this effort, terminating all federal funding for such programs,[249] with cuts also affecting organizations that support journalism and strengthen media transparency.[250]

Countering Disinformation 3 — Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public: The Trump administration canceled federally funded research grants focused on misinformation, including studies on foreign influence, AI-generated content, and disinformation tactics on social media. The move stems from Executive Order 14159, "Protecting the American People Against Invasion,"[251] aimed at protecting free speech, but critics argue its true effect is to suppress independent research into foreign influence.[252]

Countering Disinformation 4 — Create a Capability Within DHS to Actively Monitor Foreign Disinformation: The DHS has shuttered all efforts within CISA to counter foreign malign influence,[253] with the secretary arguing that CISA is "not the Ministry of Truth."[254] Elsewhere across the executive branch, the Justice Department and State Department have similarly shut down the FBI's Foreign Influence Task Force and the Global Engagement Center.[255] Despite the center's work to provide technical assistance to counter anti-American influence campaigns by U.S. adversaries abroad, Secretary Rubio celebrated its closure as a step to "liberate American speech."[256]

Countering Disinformation 5 — Create a Grant Program to Equip State and Local Governments: The Trump administration has halted all federal grant funding to support state and local governments in countering disinformation.[257] The administration has cut funding not only to the Election Infrastructure Information Sharing and Analysis Center but also to the Multi-State Information Sharing and Analysis Center because of a false perception that these organizations are involved in censorship. State and local officials have expressed concerns over cuts to federal programs,[258] with some warning that debunking politically divisive rhetoric has diverted time and resources from emergency relief efforts.[259]

Countering Disinformation 6 — Reform the Foreign Agents Registration Act and Introduce New FCC Regulations: On February 5, 2025, Attorney General Pam Bondi issued a memorandum deprioritizing Foreign Agents Registration Act (FARA) enforcement and dismantling the Justice Department's Foreign Influence Task Force and the National Security Division's Corporate Enforcement Unit.[260] This shift limits criminal cases to traditional espionage while directing the FARA Unit to focus solely on civil enforcement and injunctive relief.[261] The Justice Department's pending rulemaking from the Biden administration seeks to narrow the scope of commercial exemptions,[262] creating uncertainty for regulated entities over their future obligations and enforcement priorities.

Countering Disinformation 7 — Publish and Enforce Transparency Guidelines for Social Media Platforms: Congress has debated bills to incentivize greater transparency in social media content moderation and whether to amend Section 230 of the Communications Act of 1934, which shields platforms from liability for user-generated content and protects their ability to moderate in "good faith."[263] In 2024, Congress passed — and the Supreme Court upheld — a law requiring TikTok's Chinese parent, ByteDance, to divest or face a U.S. ban.[264] However, the Trump administration has repeatedly declined to enforce the law, allowing ByteDance to retain control of TikTok's algorithm that amplifies pro-Chinese narratives.[265] On February 20, 2025, the Federal Trade Commission launched a public inquiry to understand social media content moderation practices,[266] which could signal renewed federal engagement.

Conclusion

This assessment marks a five-year effort to track U.S. cyber policy through the lens of the commission — a period marked by geopolitical volatility, persistent fragmentation, uneven implementation, and institutional growth under pressure. While the commission's framework helped orient key reforms and catalyze action across sectors, a substantial gap between vision and execution remains. With the second Trump administration now in office, the challenge is not simply to revisit past priorities, but to confront the structural constraints that have limited progress — and to determine whether a more coherent, sustained approach to national cyber resilience is politically and institutionally viable in the years ahead.

Endnotes

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

2. U.S. Government Accountability Office, "Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization," July 30, 2025. (https://www.gao.gov/products/gao-25-108436)

3. The White House, Press Release, "Presidential Policy Directive – United States Cyber Incident Coordination," July 26, 2016. (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident)

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

5. Ibid.

6. 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)

7. Annie Fixler and Johanna Yang, "By gutting its cyber staff, State Department ignores congressional directives," *CyberScoop*, August 18, 2025. (https://cyberscoop.com/state-department-cyber-diplomacy-setback-congress-action-op-ed)

8. Notice of Termination of Discretionary Federal Advisory Committees, Department of Homeland Security, 90 Federal Register 11995, March 13, 2025. (https://www.federalregister.gov/documents/2025/03/13/2025-04011/notice-of-termination-of-discretionary-federal-advisory-committees)

9. Eric Geller, "'Suspended animation': US government upheaval has frayed partnerships with critical infrastructure," *Cybersecurity Drive*, June 25, 2025. (https://www.cybersecuritydive.com/news/critical-infrastructure-cybersecurity-partnerships-disruption-trump-government-industry/751589)

10. Weslan Hansen, "Democrats Abandon Cyber PIVOTT Bill, Citing Federal Layoffs," *MeriTalk*, February 26, 2025. (https://www.meritalk.com/articles/democrats-abandon-cyber-pivott-bill-citing-federal-layoffs)

11. 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)

12. Martin Matishak, "Exclusive: Hegseth orders Cyber Command to stand down on Russia planning," *The Record*, February 28, 2025. (http://therecord.media/hegseth-orders-cyber-command-stand-down-russia-planning)

13. @DODResponse, *X*, March 4, 2025. (https://x.com/DODResponse/status/1896960589605609627)

14. Stephanie Kirchgaessner, "Trump administration retreats in fight against Russian cyber threats," *The Guardian* (UK), March 1, 2025. (https://www.theguardian.com/us-news/2025/feb/28/trump-russia-hacking-cyber-security)

15. U.S. Department of Justice, Press Release, "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," March 5, 2025. (https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global); U.S. Department of the Treasury, Press Release, "Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks," March 5, 2025. (https://home.treasury.gov/news/press-releases/sb0042)

16. Jonathan Grieg, "Sean Cairncross confirmed as national cyber director," *The Record*, August 4, 2025. (https://therecord.media/sean-cairncross-confirmed-oncd)

17. House Appropriations Committee Democrats, Press Release, "Ranking Member Henry Cuellar Statement at the Fiscal Year 2025 Budget Request Hearing for the Cybersecurity and Infrastructure Security Agency," April 30, 2024. (https://democrats-appropriations.house.gov/news/statements/ranking-member-henry-cuellar-statement-at-the-fiscal-year-2025-budget-request-3)

18. Sam Sabin, "Exclusive: One-third of top U.S. cyber force has left since Trump took office," *Axios*, June 3, 2025. (https://www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts)

19. Tim Starks, "Contract lapse leaves critical infrastructure cybersecurity sensor data unanalyzed at national lab," *CyberScoop*, July 22, 2025. (https://cyberscoop.com/contract-lapse-leaves-critical-infrastructure-cybersecurity-sensor-data-unanalyzed-at-national-lab); Eric Geller, "'Suspended animation': US government upheaval has frayed partnerships with critical infrastructure," *Cybersecurity Drive*, June 25, 2025. (https://www.cybersecuritydive.com/news/critical-infrastructure-cybersecurity-partnerships-disruption-trump-government-industry/751589)

20. House Appropriations Committee, Appropriations Chairman Tom Cole, "Homeland Security Appropriations Act, 2026," June 8, 2025, page 6. (https://appropriations.house.gov/sites/evo-subsites/republicans-appropriations.house.gov/files/evo-media-document/fy26-homeland-security-bill-summary-full-committee.pdf)

21. Office of the Director of National Intelligence, Press Release, "DNI Gabbard Launches ODNI 2.0: Reduce bloat by over 40% and save taxpayers $700+ million per year," August 20, 2025. (https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2025/4100-pr-24-25); Office of the Director of National Intelligence, "Fact Sheet: ODNI 2.0 Launch," August 20, 2025, page 3. (https://www.dni.gov/files/ODNI/documents/ODNI-20-Fact-Sheet.pdf)

22. Office of the Director of National Intelligence, National Counterterrorism Center, "Critical Infrastructure Intelligence Initiative," January 27, 2025. (https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/241-about/organization/cyber-threat-intelligence-integration-center)

23. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Storm IX: After-Action Report," September 2024, page 16. (https://www.cisa.gov/sites/default/files/2024-10/Cyber Storm IX After-Action Report v00 20241001_508.pdf); U.S. Department of Homeland Security, Public-Private Analytic Exchange Program, "Impact of Artificial Intelligence on Criminal and Illicit Activities," September 27, 2024, pages 39-40. (https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf)

24. Leo S.F. Lin, "Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud," July 4, 2025. (https://www.mdpi.com/2075-471X/14/4/46#fn043-laws-14-00046)

25. U.S. Department of Justice, Office of the Inspector General, "Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks," September 17, 2024, pages 12-13. (https://oig.justice.gov/sites/default/files/reports/24-107.pdf)

26. Christian Vasquez, "FBI has conducted more than 30 disruption operations in 2024," *CyberScoop*, October 30, 2024. (https://cyberscoop.com/fbi-ransomware-disruption-infrastructure-cybertalks)

27. U.S. Department of Justice, Federal Bureau of Investigation, Press Release, "Joint ODNI, FBI, and CISA Statement," November 4, 2024. (https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424)

28. Cyber PIVOTT Act, H.R. 1000, 119th Congress (2025). (https://www.congress.gov/bill/119th-congress/house-bill/1000/text); Rep. Pat Fallon, Press Release, "Congressman Pat Fallon Leads Introduction of the Federal Cyber Workforce Training Act," May 16, 2025. (https://fallon.house.gov/news/documentsingle.aspx?DocumentID=1590); To amend the Cybersecurity Enhancement Act of 2014 to make improvements to the Federal Cyber Scholarship for Service Program, and for other purposes, H.R. 494, 119th Congress (2025). (https://www.congress.gov/bill/119th-congress/house-bill/494/text)

29. Maggie Miller, "State Department cyber, tech cuts deeper than previously known," *Politico*, July 17, 2025. (https://www.politico.com/news/2025/07/17/cyber-tech-state-ai-00460679); Eric Geller, "State Department cyber diplomacy firings and changes threaten US defenses," *Cybersecurity Dive*, July 17, 2025. (https://www.cybersecuritydive.com/news/state-department-cyber-bureau-firings-reorganization/753370); Dana Nickel, "Trump's slash-and-burn agenda hits DOD's cyber workforce," *Politico*, May 27, 2025. (https://www.politico.com/newsletters/weekly-cybersecurity/2025/05/27/trumps-slash-and-burn-agenda-hits-dods-cyber-workforce-00369889)

30. Jiwon Ma and Mark Montgomery, "2023 Annual Report on Implementation," *CSC 2.0*, September 19, 2023, page 6. (https://cybersolarium.org/wp-content/uploads/2023/09/CSC2.0_Report_2023AnnualReport.pdf)

31. U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview Fiscal Year 2026 Congressional Justification," June 17, 2025, page 34. (https://www.dhs.gov/sites/default/files/2025-06/25_0613_cisa_fy26-congressional-budget-justificatin.pdf)

32. 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)

33. Martin Matishak, "Cyber diplomacy funding halted as US issues broad freeze on foreign aid," *The Record*, January 25, 2025. (https://therecord.media/cyber-diplomacy-funding-halted-freeze-on-foreign-aid)

34. Maggie Miller, "State Department cyber, tech cuts deeper than previously known," *Politico*, July 17, 2025. (https://subscriber.politicopro.com/article/2025/07/state-department-cyber-tech-cuts-wider-than-previously-known-00460679)

35. U.S. Department of State, "New Org Chart," July 1, 2025, page 1. (https://www.state.gov/wp-content/uploads/2025/04/DOS-Reorg-4.21.2025.pdf); U.S. Department of State, "United States Department of State Org Chart," June 2024, page 1. (https://www.state.gov/wp-content/uploads/2024/06/DOS-Org-Chart-Accessible-Template-May-2024.pdf); Dani Schulkin, Tess Bridgeman, and Andrew Miller, "What Just Happened: The Trump Administration's Reorganization of the State Department – and How We Got Here," *Just Security*, April 22, 2025. (https://www.justsecurity.org/110772/wjh-trump-reorganization-state-department)

36. Sen. Marco Rubio, "Why Protests Matter: The Battle Between Authoritarianism and Democracy, a War We Must Win," *Journal of International Affairs*, October 29, 2020. (https://jia.sipa.columbia.edu/news/why-protests-matter-battle-between-authoritarianism-and-democracy-war-we-must-win)

37. Rose Payne, "The OEWG ends and a new UN cybersecurity permanent mechanism is born," *Global Partners Digital*, July 24, 2025. (https://www.gp-digital.org/the-oewg-ends-and-a-new-un-cybersecurity-permanent-mechanism-is-born)

38. Alexandra Kelley and Eric Katz, "NIST fires over 70 probationary employees," *NextGov/FCW*, March 4, 2025. (https://www.nextgov.com/people/2025/03/nist-fires-over-70-probationary-employees/403459); David Dimolfetta, "State Department cuts hit cyber diplomats doing international engagements," *NextGov/FCW*, July 15, 2025. (https://www.nextgov.com/people/2025/07/state-department-cuts-hit-cyber-diplomats-doing-international-engagements/406727); Eric Geller, "Trump proposes major cut to CISA's budget, citing false 'censorship' claims," *Cybersecurity Dive*, May 2, 2025. (https://www.cybersecuritydive.com/news/trump-cisa-budget-cuts-disinformation/747047)

39. Blake Ledbetter and Drew Clark, "Trump Says Tariff Threat Drove U.S. Investments, Blasts Biden on Energy," *Broadband and Breakfast*, March 5, 2025. (https://broadbandbreakfast.com/trump-criticizes-biden-touts-ai-and-core-energy-in-joint-address-2)

40. Cathy Fang, "What a US Exit From the Information Technology Agreement Would Mean for America and the World," *The Diplomat*, April 14, 2025. (https://thediplomat.com/2025/04/what-the-us-exit-from-the-information-technology-agreement-means-for-america-and-the-world)

41. Michael Igoe, "Exclusive: State Department issues stop-work order on US aid," *Devex*, January 24, 2025. (https://www.devex.com/news/exclusive-state-department-issues-stop-work-order-on-us-aid-109160)

42. @marcorubio, *X*, March 10, 2025. (https://x.com/marcorubio/status/1899021361797816325?lang=en); Sam Mednick, Wilson McMakin, and Monika Pronczuk, "USAID cuts are already hitting countries around the world. Here are 20 projects that have closed," *Associated Press*, March 1, 2025. (https://apnews.com/article/usaid-cuts-hunger-sickness-288b1d3f80d85ad749a6d758a778a5b2)

43. Annie Fixler and Johanna Yang, "USAID Cuts Demolish Cyber Assistance to U.S. Allies and Partners," *Cipher Brief*, March 17, 2025. (https://www.thecipherbrief.com/column_article/usaid-cuts-demolish-cyber-assistance-to-u-s-allies-and-partners)

44. U.S. Department of Justice, Federal Bureau of Investigation, Press Release, "FBI Opens Standalone Office in New Zealand," July 31, 2025. (https://www.fbi.gov/news/press-releases/fbi-opens-standalone-office-in-new-zealand)

45. U.S. Department of Justice, Justice Management Division, "Fiscal year 2026 Budget and Performance Summary," June 13, 2025, page 133 (https://www.justice.gov/media/1403736/dl)

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://bidenwhitehouse.archives.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, "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 9, 2024. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/09/09/press-release-notice-on-the-continuation-of-the-national-emergency-with-respect-to-foreign-interference-in-or-undermining-public-confidence-in-united-states-elections-2)

47. U.S. Department of the Treasury, Press Release, "Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks," March 5, 2025. (https://home.treasury.gov/news/press-releases/sb0042)

48. Jonathan Greig, "NSA: Volt Typhoon was 'not successful' at persisting in critical infrastructure," *The Record*, July 15, 2025. (https://therecord.media/china-typhoon-hackers-nsa-fbi-response)

49. Allison Pytlak, "Cyber Diplomacy 2.0: From Process to Impact," *Stimson Center*, August 4, 2025. (https://www.stimson.org/2025/cyber-diplomacy-2-0-from-process-to-impact)

50. Annie Fixler and Johanna Yang, "By gutting its cyber staff, State Department ignores congressional directives," *CyberScoop*, August 18, 2025. (https://cyberscoop.com/state-department-cyber-diplomacy-setback-congress-action-op-ed)

51. 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)

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

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

54. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "DHS Launches Over $100 Million in Funding to Strengthen Communities' Cyber Defenses," August 1, 2025. (https://www.cisa.gov/news-events/news/dhs-launches-over-100-million-funding-strengthen-communities-cyber-defenses); Kevin Kinnally, "FEMA's Preparedness Grants Come with New Strings — and Delays," *Maryland Association of Counties*, August 6, 2025. (https://conduitstreet.mdcounties.org/2025/08/06/femas-preparedness-grants-come-with-new-strings-and-delays)

55. 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)

56. Samantha Ravich, "Continuity of the Economy," *The Republic*, May 8, 2025. (https://therepublicjournal.com/essays/continuity-of-the-economy)

57. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1267. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=839)

58. U.S. House Committee on Financial Services, Chairman French Hill, Press Release, "Davidson: The DPA Is A Critical Component Of The United States' National Security Toolkit That Warrants Reauthorization," June 12, 2025. (https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409769)

59. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "National Cyber Incident Response Plan Public Comment Draft," December 2024. (https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-update-public-comment-draft)

60. 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#page=519)

61. U.S. Department of Homeland Security, "FY 2025 Budget in Brief," March 11, 2024, page 106. (https://www.dhs.gov/sites/default/files/2024-04/2024_0311_fy_2025_budget_in_brief.pdf#page=113); U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview Fiscal Year 2026 Congressional Justification," June 9, 2025, page 81. (https://www.dhs.gov/sites/default/files/2025-06/25_0613_cisa_fy26-congressional-budget-justificatin.pdf#page=97)

62. 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)

63. U.S. Southern Command, "Cyber Exercise Southern Defender 2025 Bolsters Partner Nation Defense Capabilities," May 12, 2025. (https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/4181288/cyber-exercise-southern-defender-2025-bolsters-partner-nation-defense-capabilit); U.S. Embassy in Romania, Press Release, "Maryland National Guard Cyber Forces and the Romanian Cyber Defense Command Strengthen NATO's Resilient Cyber Defense in Saber Guardian 25," June 17, 2025. (https://ro.usembassy.gov/maryland-national-guard-cyber-forces-and-the-romanian-cyber-defense-command-strengthen-natos-resilient-cyber-defense-in-saber-guardian-25); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Storm IX: After-Action Report," September 2024, page 31. (https://www.cisa.gov/sites/default/files/2024-10/Cyber Storm IX After-Action Report v00 20241001_508.pdf)

64. William T. Adler, Doug Chapin, Krysha Gregorowicz, Lily Kincannon, Julianne Lempert, Theo Menon, Lindsay Nielson, Rachel Orey, and David Varas Alonso, "Measuring the Impact of Recent Grants to Election Administrators Under the Help America Vote Act," *Bipartisan Policy Center*, January 30, 2025, page 2. (https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2025/01/BPC_Election-Security-Grant-report_R04-1.pdf)

65. House Appropriations Committee Democrats, "Financial Services and General Government," July 20, 2025, page 3. (https://democrats-appropriations.house.gov/sites/evo-subsites/democrats-appropriations.house.gov/files/evo-media-document/fy26-financial-services-and-general-government-summary.pdf); U.S. Election Assistance Commission, "Fiscal Year 2026 Congressional Budget Justification," May 30, 2025, page 5. (https://www.eac.gov/sites/default/files/2025-05/FISCAL_YEAR_2026_EAC_CONGRESSIONAL_BUDGET_JUSTIFICATION.pdf)

66. Colin Wood, "Federal cuts to information-sharing groups may damage nation's security posture, warn officials," *StateScoop*, March 13, 2025. (https://statescoop.com/eiisac-msisac-center-internet-security-cisa-cuts-2025)

67. U.S. Federal Election Committee, Press Release, "FEC approves two advisory opinions, Final Rule on candidate security, notice of disposition of rulemaking, and interpretive rule," September 19, 2024. (https://www.fec.gov/updates/fec-approves-two-advisory-opinions-final-rule-on-candidate-security-notice-of-disposition-of-rulemaking-and-interpretive-rule); U.S. Federal Election Committee, Press Release, "Commission approves regulations regarding use of campaign funds for candidate and officeholder security," September 25, 2024. (https://www.fec.gov/updates/commission-approves-regulations-regarding-use-of-campaign-funds-for-candidate-and-officeholder-security); Derek B. Johnson, "FEC expands campaign spending rules to allow for physical, cybersecurity purchases," *CyberScoop*, September 24, 2024. (https://cyberscoop.com/fec-campaign-funds-security-purchases)

68. Barbara Ortutay and Claire Rush, "The Digital Equity Act tried to close the digital divide. Trump calls it racist and acts to end it," *Associated Press*, May 25, 2025. (https://apnews.com/article/digital-equity-act-trump-broadband-rural-diversity-90d1c8a618d289ecb16e1667194e37d7); Seamus Dowdall, "NTIA terminates Digital Equity Act grants," *National Association of Counties*, May 14, 2025. (https://www.naco.org/news/ntia-terminates-digital-equity-act-grants)

69. Keely Quinlan, "State, local organizations ask Commerce Dept. to reinstate Digital Equity Act," *StateScoop*, June 20, 2025. (https://statescoop.com/state-local-commerce-ntia-reinstate-digital-equity-act); George Winslow, "Charter Awards $1.3M in 2024 Spectrum Digital Education Grants," *TvTech*, September 20, 2024. (https://www.tvtechnology.com/news/charter-awards-dollar13m-in-2024-spectrum-digital-education-grants)

70. Office of the Director of National Intelligence, "Foreign Threats to US Election After Voting Ends in 2024," October 8, 2024, page 1. (https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Foreign-Threats-to-US-Elections-After-Voting-Ends-in-2024.pdf)

71. Ari Ben Am and Johanna Yang, "China and Russia Rejoice as the U.S. Cuts Its Global Media," *National Interest*, April 13, 2025. (https://nationalinterest.org/feature/authoritarians-rejoice-as-the-u-s-cuts-its-global-media)

72. White House, Press Release, "White House Launches "U.S. Cyber Trust Mark", Providing American Consumers an Easy Label to See if Connected Devices are Cybersecure," January 7, 2025. (https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure)

73. Brian Flood, "Trump-appointed FCC chairman probes Biden cybersecurity program over China concerns," *Fox News*, June 19, 2025. (https://www.foxnews.com/media/trumps-fcc-probes-biden-admin-cyber-trust-mark-initiative-over-concerns-about-deep-ties-china)

74. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=960)

75. Alexandra Kelley and Eric Katz, "NIST fires over 70 probationary employees," *NextGov/FCW*, March 4, 2025. (https://www.nextgov.com/people/2025/03/nist-fires-over-70-probationary-employees/403459)

76. Justin Doubleday, "House appropriators reject NIST funding cuts," *Federal News Network*, July 15, 2025. (https://federalnewsnetwork.com/congress/2025/07/nist-to-get-funding-boost-under-house-bill)

77. The White House, "Major Discretionary Funding Changes," May 2, 2025, page 25. (https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf)

78. House Appropriations Committee, "Department of Commerce and Justice, Science, and Related Agencies Appropriations Bill, 2026," July 14, 2025, page 4. (https://appropriations.house.gov/sites/evo-subsites/republicans-appropriations.house.gov/files/evo-media-document/fy26-commerce,-justice,-science,-and-related-agencies-bill-summary-subcommittee.pdf); Senate Appropriations Committee, "Department of Commerce and Justice, Science, and Related Agencies Appropriations Bill, 2026, Report," July 17, 2025, page 29. (https://www.appropriations.senate.gov/imo/media/doc/fy26_cjs_senate_report.pdf)

79. "Cyber Strategies and Successes: A Conversation with National Cyber Director Harry Coker, Jr," *Foundation for Defense of Democracies*, January 7, 2025, page 5. (https://www.fdd.org/wp-content/uploads/2025/01/FDDEvent_CyberStrategiesandSuccessesAConversationwithNationalCyberDirectorHarryCokerJr_Transcript-1.pdf)

80. U.S. Executive Order 14144, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," January 16, 2025. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity)

81. U.S. Executive Order 13694, "Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144," June 6, 2025. (https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144)

82. U.S. Department of Commerce, National Institute of Standards and Technology, "Statistics Results," accessed August 9, 2025. (https://nvd.nist.gov/vuln/search#/nvd/home?vulnRevisionStatusList=awaiting_analysis&resultType=statistics)

83. "Infrastructure Security in the Cyber Age: A Conversation with CISA Director Jen Easterly," *Foundation for Defense of Democracies*, January 15, 2025, page 14. (https://www.fdd.org/wp-content/uploads/2025/01/FDD-Event_InfrastructureSecurityintheCyberAgeAConversationwithCISADirectorJenEasterly_Transcript.pdf)

84. Hansi Lo Wang, "The public lost access to Census Bureau data for days after a Trump order," *NPR*, February 12, 2025. (https://www.npr.org/2025/02/12/nx-s1-5289329/us-census-bureau-survey-data)

85. Ben Casselman, "Trump Fired America's Economic Data Collector. History Shows the Perils," *The New York Times*, August 3, 2025. (https://www.nytimes.com/2025/08/03/business/trump-bls-firing-economic-reports.html)

86. National Association of Insurance Commissioners, "Implementation of Model Act #668 Insurance Data Security Model Law [status as of May 2, 2025]," accessed August 12, 2025, page 2. (https://content.naic.org/sites/default/files/government-affairs-brief-data-security-model-law.pdf); National Association of Insurance Commissioners, "Implementation of Model Act #668 Insurance Data Security Model Law [status as of August 8, 2025]," accessed August 12, 2025, page 1. (https://content.naic.org/sites/default/files/cmte-h-cybersecurity-wg-state-adoption-map-model-668.pdf)

87. Ian Smith, "Insurance groups urge state support for 'uninsurable' cyber risks," *Financial Times* (UK), September 4, 2024. (https://www.ft.com/content/c2769c6d-8bec-4167-af5c-53c6cf139851)

88. National Association of Insurance Commissioners, "NAIC Federal Financial Priorities Letter to Congress," March 21, 2025, page 3. (https://content.naic.org/sites/default/files/naic2025federalfinancialprioritiesletter.pdf)

89. U.S. Department of Commerce, National Institute of Standards and Technology, "NIST IR 8286A Rev. 1 (Initial Public Draft), Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management," February 26, 2025. (https://csrc.nist.gov/pubs/ir/8286/a/r1/ipd); Stephen Quinn, Nahla Ivy, Matthew Barrett, Larry Feldman, Greg Witte, and R.K. Gardner, "NIST Interagency Report NIST IR 8286Ar1 ipd, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management," *National Institute of Standards and Technology*, February 26, 2025, pages 28-30 and 37. (https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8286Ar1.ipd.pdf)

90. 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)

91. U.S. Department of Homeland Security, "Cyber Risk Economics," August 2, 2024. (https://www.dhs.gov/archive/science-and-technology/cyrie); Andrew Morin, "UTulsa Cyber Studies professors secure $600,000 NSF grant for pioneering cybersecurity research project," *University of Tulsa*, June 19, 2025. (https://utulsa.edu/news/utulsa-cyber-studies-professors-secure-600000-nsf-grant-for-pioneering-cybersecurity-research-project); U.S. Department of the Treasury, Federal Insurance Office, "Industry-University Cooperative Research Center for Terrorism and Catastrophic Cyber Insurance Modeling and Underwriting," accessed August 12, 2025. (https://home.treasury.gov/system/files/311/IUCRC FACI Presentation FINAL.pdf)

92. Sasha Romanosky, Lloyd Dixon, R.J. Briggs, and Henry H. Willis, "Insuring Catastrophic Cyber Risk," *RAND*, June 9, 2025. (https://www.rand.org/pubs/research_reports/RRA3817-1.html); Nick Leiserson, "How a Government Reinsurance Program Can Accelerate Maturation of the Cyber Insurance Market," *Foundation for Defense of Democracies*, June 17, 2025. (https://www.fdd.org/analysis/2025/06/17/how-a-government-reinsurance-program-can-accelerate-maturation-of-the-cyber-insurance-market)

93. U.S. Executive Order 14275, "Restoring Common Sense to Federal Procurement," April 15, 2025. (https://www.whitehouse.gov/presidential-actions/2025/04/restoring-common-sense-to-federal-procurement)

94. 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)

95. U.S. Office of Management and Budget, "Modernizing the Federal Risk and Authorization Management Program (FedRAMP)," July 25, 2024, page 1. (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf)

96. Miranda Nazzaro, "FedRAMP authorizations in 2025 already more than double last year, GSA says," *FedScoop*, August 11, 2025. (https://fedscoop.com/fedramp-government-cloud-services-technology-modernization)

97. Caroline Nihill and Rebecca Heilweil, "GSA unveils FedRAMP revamp with automation, private sector in mind," *FedScoop*, March 24, 2025. (https://fedscoop.com/gsa-fedramp-20x-automation-private-sector)

98. U.S. General Services Administration, Press Release, "GSA Celebrates Major Milestones in FedRAMP Cloud Authorization Reform," August 11, 2025. (https://www.gsa.gov/about-us/newsroom/news-releases/gsa-celebrates-major-fedramp-milestones-08112025); Billy Mitchell, "GSA inks governmentwide deal with AWS, touting $1B in potential savings," *FedScoop*, August 7, 2025. (https://fedscoop.com/aws-gsa-onegov-deal-1-billion-savings)

99. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=844); U.S. Government Accountability Office, "Cybersecurity: DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security," April 29, 2025. (https://www.gao.gov/products/gao-25-107313)

100. The White House, Office of the National Cyber Director, Press Release, "Press Release: White House Office of the National Cyber Director Releases Roadmap to Enhance Internet Routing Security," September 3, 2024. (https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/09/03/press-release-white-house-office-of-the-national-cyber-director-releases-roadmap-to-enhance-internet-routing-security); The White House, Office of the National Cyber Director, "Roadmap to Enhancing Internet Routing Security," September 3, 2024. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf)

101. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "#StopRansomware: Interlock," July 22, 2025, pages 1-2. (https://www.cisa.gov/sites/default/files/2025-07/aa25-203a-stopransomware-interlock-072225.pdf)

102. U.S. Department of Commerce, National Institute of Standards and Technology, "NIST SP 800-189 Rev. 1 (Initial Public Draft) Border Gateway Protocol Security and Resilience," January 3, 2025 (https://csrc.nist.gov/pubs/sp/800/189/r1/ipd); Kotikalapudi Sriram and Doug Montgomery, "NIST Special Publication 800 NIST SP 800-189r1 ipd, Border Gateway Protocol Security and Resilience," *National Institute of Standards and Technology*, January 3, 2025. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189r1.ipd.pdf)

103. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services," December 17, 2024. (https://www.cisa.gov/news-events/directives/bod-25-01-implementation-guidance-implementing-secure-practices-cloud-services)

104. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, "People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," September 28, 2024, pages 1-3. (https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF)

105. U.S. Department of State, Press Release, "Sanctioning PRC Cyber Company Involved in Malicious Botnet Operations," January 3, 2025. (https://2021-2025.state.gov/sanctioning-prc-cyber-company-involved-in-malicious-botnet-operations)

106. U.S. Department of Justice, Northern District of Oklahoma Attorney's Office, Press Release, "Botnet Dismantled in International Operation, Russian and Kazakhstani Administrators Indicted," May 9, 2025. (https://www.justice.gov/usao-ndok/pr/botnet-dismantled-international-operation-russian-and-kazakhstani-administrators)

107. 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)

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

109. U.S. International Trade Administration, "Germany Country Commercial Guide," August 1, 2025. (https://www.trade.gov/country-commercial-guides/germany-information-and-communications-technology-ict)

110. U.S. Department of Commerce, National Telecommunications and Information Administration, Press Release, "More than 90 Applications Requesting Nearly $3 Billion Submitted for the Wireless Innovation Fund's Third Round," May 8, 2025. (https://www.ntia.gov/press-release/2025/more-90-applications-requesting-nearly-3-billion-submitted-wireless-innovation-fund-s-third-round)

111. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1478. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf#page=114)

112. U.S. Department of Commerce, National Institute of Standards and Technology, "Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems," June 4, 2025. (https://csrc.nist.gov/pubs/sp/800/18/r2/ipd)

113. "Tracking the Progress of the CHIPS R&D Initiatives," *Semiconductor Industry Association*, March 12, 2025. (https://www.semiconductors.org/chips-rd-programs)

114. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1576. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf#page=212); Ibid., 136 Stat. 1584.

115. Emily Kwong, Rachel Carlson, Rob Stein, Pien Huang, Jonathan Lambert, Gisele Grayson, and Rebecca Ramirez, "How the Trump administration is halting scientific research," *NPR*, March 11, 2025. (https://www.npr.org/2025/03/11/1266983351/trump-science-medical-research-layoffs)

116. Jeremy W. Peters and Andrea Fuller, "How Universities Became So Dependent on the Federal Government," *The New York Times*, April 18, 2025. (https://www.nytimes.com/2025/04/18/us/trump-universities.html); Nina Pasquini, "Harvard Research on Halt," *Harvard Magazine*, April 18, 2025. (https://www.harvardmagazine.com/2025/04/harvard-research-funding-freeze); Benjamin Mueller, "Trump Administration Has Begun a War on Science, Researchers Say," *The New York Times*, March 31, 2025. (https://www.nytimes.com/2025/03/31/science/trump-science-nas-letter.html)

117. Organisation for Economic Co-operation and Development, "R&D spending growth slows in OECD, surges in China; government support for energy and defence R&D rises sharply," March 31, 2025. (https://www.oecd.org/en/data/insights/statistical-releases/2025/03/rd-spending-growth-slows-in-oecd-surges-in-china-government-support-for-energy-and-defence-rd-rises-sharply.html)

118. U.S. Executive Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," September 15, 2022. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states)

119. U.S. Department of the Treasury, Press Release, "Treasury Issues Final Rule Expanding CFIUS Coverage of Real Estate Transactions Around More Than 60 Military Installations," November 1, 2024. (https://home.treasury.gov/news/press-releases/jy2708)

120. U.S. Department of the Treasury, Committee on Foreign Investment in the United States, "Annual Report to Congress Report Period: CY 2024," August 6, 2025, page 5. (https://home.treasury.gov/system/files/206/2024-CFIUS-Annual-Report.pdf)

121. U.S. Department of Homeland Security, "Termination of Current Membership," January 20, 2025. (https://www.documentcloud.org/documents/25500121-dhs-letter-on-termination-of-all-dhs-advisory-committee-members)

122. House Energy and Commerce, Chairman Brett Guthrie, Press Release, "Chairman Guthrie and Vice Chairman Joyce Announce Creation of Privacy Working Group," February 12, 2025. (https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-announce-creation-of-privacy-working-group)

123. U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries," April 11, 2025. (https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive); U.S. Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," February 28, 2024. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern)

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

125. Eric Geller, "'Suspended animation': US government upheaval has frayed partnerships with critical infrastructure," *Cybersecurity Dive*, June 25, 2025. (https://www.cybersecuritydive.com/news/critical-infrastructure-cybersecurity-partnerships-disruption-trump-government-industry/751589)

126. Tim Starks, "'Whatever we did was not enough': How Salt Typhoon slipped through the government's blind spots," *CyberScoop*, May 20, 2025. (https://cyberscoop.com/salt-typhoon-us-government-response)

127. U.S. Government Accountability Office, "Cybersecurity: Implementation of the 2015 Information Sharing Act," July 10, 2025, pages 1-2. (https://www.gao.gov/assets/gao-25-108509.pdf)

128. Kevin Poireault, "#BHUSA: CISA Execs 'Hopeful' for Extension of Cybersecurity Information Sharing Act," *Infosecurity Magazine*, August 8, 2025. (https://www.infosecurity-magazine.com/news/cisa-cybersecurity-information)

129. Maggie Miller and Dana Nickel, "Government flying partially blind to threats after key cyber law expires," *Politico*, October 3, 2025. (https://www.politico.com/news/2025/10/03/cyber-law-cisa-2015-shutdown-00592501)

130. Matt Kapko, "Amazon, CrowdStrike, Google and Palo Alto Networks claim no change to threat intel sharing under Trump," *CyberScoop*, May 2, 2025. (https://cyberscoop.com/public-private-threat-intel-sharing-trump-admin)

131. Office of the Director of National Intelligence, National Counterterrorism Center, "Critical Infrastructure Intelligence Initiative," January 27, 2025. (https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/241-about/organization/cyber-threat-intelligence-integration-center)

132. 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)

133. Jonathan Grieg, "CISA pledges to continue backing CVE Program after April funding fiasco," *The Record*, August 8, 2025. (https://therecord.media/cisa-pledges-support-cve-program-black-hat)

134. Tim Starks, "'Whatever we did was not enough': How Salt Typhoon slipped through the government's blind spots," *CyberScoop*, May 20, 2025. (https://cyberscoop.com/salt-typhoon-us-government-response)

135. Eric Geller, "Trump's CISA budget lays out deep job cuts, program reductions," *Cybersecurity Drive*, June 2, 2025. (https://www.cybersecuritydive.com/news/cisa-trump-2026-budget-proposal/749539)

136. House Appropriations Committee, "Department of Homeland Security Appropriations Bill, 2026, Report," pages 68-69. (https://docs.house.gov/meetings/AP/AP00/20250624/118429/HMKP-119-AP00-20250624-SD002.pdf)

137. 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#page=521)

138. Tim Starks, "Contract lapse leaves critical infrastructure cybersecurity sensor data unanalyzed at national lab," *CyberScoop*, July 22, 2025. (https://cyberscoop.com/contract-lapse-leaves-critical-infrastructure-cybersecurity-sensor-data-unanalyzed-at-national-lab)

139. 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)

140. 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)

141. "Infrastructure Security in the Cyber Age: A Conversation with CISA Director Jen Easterly," *Foundation for Defense of Democracies*, January 15, 2025, page 14. (https://www.fdd.org/wp-content/uploads/2025/01/FDD-Event_InfrastructureSecurityintheCyberAgeAConversationwithCISADirectorJenEasterly_Transcript.pdf)

142. James Rundle, "Cyber Reporting Rules Savaged in House Hearing," *The Wall Street Journal*, March 12, 2025. (https://www.wsj.com/articles/cyber-reporting-rules-savaged-in-house-hearing-fdb3e39b)

143. 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)

144. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "2024 Year In Review." (https://www.cisa.gov/about/2024YIR)

145. Office of the Director of National Intelligence, National Counterterrorism Center, "Critical Infrastructure Intelligence Initiative," January 27, 2025. (https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/241-about/organization/cyber-threat-intelligence-integration-center); National Security Agency, Central Security Service, Press Release, "NSA and Others Publish Guidance for Secure OT Product Selection," January 13, 2025. (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4027075/nsa-and-others-publish-guidance-for-secure-ot-product-selection); National Security Agency, "NSA News & Highlights," June 30, 2025. (https://www.nsa.gov/Press-Room/News-Highlights/Tag/55841/cybersecurity)

146. 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)

147. Jonathan Greig, "CISA releases first draft of updated National Cyber Incident Response Plan," *The Record*, December 16, 2024. (https://therecord.media/cisa-first-draft-updated-cyber-plan)

148. Eric Geller, "'People Are Scared': Inside CISA as It Reels From Trump's Purge," *WIRED*, March 13, 2025. (https://www.wired.com/story/inside-cisa-under-trump)

149. Eric Geller, "CISA's Joint Cyber Defense Collaborative takes major personnel hit," *Cybersecurity Drive*, July 30, 2025. (https://www.cybersecuritydive.com/news/cisa-joint-cyber-defense-collaborative-contract-lapse/756231)

150. 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)

151. U.S. Department of Defense, Office of the Secretary of Defense, Defense Business Board, "Industry Partnerships for Crises," November 12, 2024, pages 4-5. (https://dbb.defense.gov/Portals/35/Documents/Reports/2025/Industry Partnerships for Crises Study Report_CLEARED_ 22 Nov_red.pdf); Acting Assistant Secretary of Defense for Cyber Policy Laurie Buckhout, "Fiscal Year 2026 Review of the Department of Defense's Cyber Posture," *Testimony before the U.S. House Armed Services Committee, Subcommittee on Cybersecurity, Innovation, Technologies, and Information Systems*, May 16, 2025, page 8. (https://armedservices.house.gov/uploadedfiles/5.16_buckhout_written_testimony.pdf)

152. 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#page=492); Ibid., 135 Stat. 2064.

153. National Defense Authorization Act for Fiscal Year 2025, Pub. L. 118-159, 138 Stat. 2149. (https://www.congress.gov/118/plaws/publ159/PLAW-118publ159.pdf#page=377)

154. Center for Strategic and International Studies, Press Release, "CSIS Launches Commission on Cyber Force Generation," August 4, 2025. (https://www.csis.org/news/csis-launches-commission-cyber-force-generation)

155. U.S. Department of Defense, Office of the Under Secretary of Defense Comptroller, "Department of Defense DD 1414 Base for Reprogramming Actions Division A of Public Law 119-4, Full-Year Continuing Appropriations Act, 2025," April 18, 2025, page 240. (https://comptroller.defense.gov/Portals/45/Documents/execution/FY_2025_DD_1414_Base_for_Reprogramming_Actions.pdf#page=240)

156. Acting Assistant Secretary of Defense for Cyber Policy Laurie Buckhout, "Fiscal Year 2026 Review of the Department of Defense's Cyber Posture," *Testimony before the U.S. House Armed Services Committee, Subcommittee on Cybersecurity, Innovation, Technologies, and Information Systems*, May 16, 2025, page 8. (https://armedservices.house.gov/uploadedfiles/5.16_buckhout_written_testimony.pdf)

157. Mark Pomerleau, "Cyber Command significantly increases funding request for defense in Indo-Pacific region, *DefenseScoop*, July 1, 2025. (https://defensescoop.com/2025/07/01/cyber-command-2026-budget-request-increase-funding-indo-pacific-defense)

158. 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)

159. 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)

160. U.S. House Armed Services Committee, "Department of Defense Fiscal Year 2026 Budget Request" June 12, 2025. (https://www.youtube.com/live/PmB8OW_cbS8?si=N5rApOFCHADlLjo-&t=7619)

161. National Defense Authorization Act for Fiscal Year 2026, S. 2296, 119th Congress (2025), Section 1610A. (https://www.congress.gov/bill/119th-congress/senate-bill/2296/text); Rep. Don Bacon, Press Release, "Bacon Lauds Progress on FY26 Defense Policy Bill," July 16, 2025. (https://bacon.house.gov/news/documentsingle.aspx?DocumentID=2726)

162. U.S. Cyber Command, Press Release, "Posture Statement of Lieutenant General William J. Hartman," April 9, 2025. (https://www.cybercom.mil/Media/News/Article/4150133/posture-statement-of-lieutenant-general-william-j-hartman)

163. 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)

164. U.S. Government Accountability Office, "Space Operations DoD Is Pursuing Efforts to Collaborate with Allies and Partners but Needs to Address Key Challenges," July 8, 2025, pages 1 and 4. (https://www.gao.gov/assets/gao-25-108043.pdf)

165. 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)

166. National Defense Authorization Act for Fiscal Year 2026, S. 2296, 119th Congress (2025), Section 1605. (https://www.congress.gov/bill/119th-congress/senate-bill/2296/text)

167. 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)

168. U.S. Department of Defense, Press Release, "Diba Hadi Announced as the Principal Director, Cyber Academic Engagement Office," August 30, 2024. (https://www.defense.gov/News/Releases/Release/Article/3891116/diba-hadi-announced-as-the-principal-director-cyber-academic-engagement-office)

169. Jordan McDonald, "DOD's Cyber Academic Engagement Office Centralizes Operations to Drive Efficiency," *GovCIO*, March 31, 2025. (https://govciomedia.com/dods-cyber-academic-engagement-office-centralizes-operations-to-drive-efficiency)

170. 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); 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=546); 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); U.S. Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-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://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems)

171. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 542. (https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=408)

172. Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Activities, Office of the Secretary, Department of Defense, 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)

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

174. "Jon Harper, "DOD Cyber Crime Center's vulnerability disclosure program racking up savings for industrial base," *DefenseScoop*, October 30, 2024. (https://defensescoop.com/2024/10/30/dc3-defense-industrial-base-vulnerability-disclosure-program-dib-vdp)

175. Lisbeth Perez, "New NSA AI Tool to Automate Cyber Threat Detection," *MeriTalk*, November 29, 2024. (https://www.meritalk.com/articles/new-nsa-ai-tool-to-automate-cyber-threat-detection)

176. 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)

177. Mikayla Easley, "DOD releases final rule for CMMC, setting the stage for implementation next year," *DefenseScoop*, October 11, 2024. (https://defensescoop.com/2024/10/11/dod-cmmc-final-rule-cybersecurity-standards-contractors)

178. 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#page=506)

179. 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)

180. 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)

181. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. 118-159, 138 Stat. 1837, 138 Stat. 1848, and 138 Stat. 2118. (https://www.congress.gov/118/plaws/publ159/PLAW-118publ159.pdf)

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

183. U.S. Government Accountability Office, "Cybersecurity: DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security," April 29, 2025. (https://www.gao.gov/products/gao-25-107313)

184. Sophie McDowall and Mark Montgomery, "Washington limits states' access to critical cyber resources," *The Washington Examiner*, August 17, 2025. (https://www.washingtonexaminer.com/op-eds/3501377/washington-limits-states-access-critical-cyber-resources-trump-cisa)

185. White House, Press Release, "White House Launches 'U.S. Cyber Trust Mark', Providing American Consumers an Easy Label to See if Connected Devices are Cybersecure," January 7, 2025. (https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure)

186. Brian Flood, "Trump-appointed FCC chairman probes Biden cybersecurity program over China concerns," *Fox News*, June 19, 2025. (https://www.foxnews.com/media/trumps-fcc-probes-biden-admin-cyber-trust-mark-initiative-over-concerns-about-deep-ties-china)

187. Keely Quinlan, "Collaboration was key to nation's most 'cyber-secure' election to date," *StateScoop*, December 11, 2024. (https://statescoop.com/cybersecurity-secure-election-day-2024)

188. Center for Internet Security, "In response to federal funding cuts, the EI-ISAC Executive Committee is exploring options to continue its vital support to election offices," accessed August 16, 2025. (https://www.cisecurity.org/ei-isac)

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

190. U.S. Executive Order 14149, "Restoring Freedom of Speech and Ending Federal Censorship," January 20, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship)

191. Keely Quinlan, "Collaboration was key to nation's most 'cyber-secure' election to date," *StateScoop*, December 11, 2024. (https://statescoop.com/cybersecurity-secure-election-day-2024); Center for Internet Security, "In response to federal funding cuts, the EI-ISAC Executive Committee is exploring options to continue its vital support to election offices," accessed August 16, 2025. (https://www.cisecurity.org/ei-isac)

192. 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)

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

194. Tim Starks, "National Cyber Director Harry Coker looks back (and ahead) on the Cyber Director office," *CyberScoop*, January 7, 2025. (https://cyberscoop.com/national-cyber-director-harry-coker-looks-back-and-ahead-on-the-cyber-director-office)

195. The White House, Press Release, "U.S. Senate Confirms Sean Cairncross as the National Cyber Director," August 2, 2025. (https://www.whitehouse.gov/briefings-statements/2025/08/u-s-senate-confirms-sean-cairncross-as-the-national-cyber-director)

196. "Cyber Strategies and Successes: A Conversation with National Cyber Director Harry Coker, Jr," *Foundation for Defense of Democracies*, January 7, 2025, page 7. (https://www.fdd.org/wp-content/uploads/2025/01/FDDEvent_CyberStrategiesandSuccessesAConversationwithNationalCyberDirectorHarryCokerJr_Transcript-1.pdf)

197. 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://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

198. Grace Dille, "OPM's 'Merit' Hiring Plan Targets STEM, Early Career Talent," *MeriTalk*, May 30, 2025. (https://www.meritalk.com/articles/opms-merit-hiring-plan-targets-stem-early-career-talent); U.S. Office of Personnel Management, "Federal Rotational Cyber Workforce Program," accessed August 21, 2025. (https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/federal-rotational-cyber-workforce-program)

199. U.S. Department of Labor, Press Release, "US Department of Labor Awards Nearly $84m in Grants to Expand Registered Apprenticeships," June 30, 2025. (https://www.dol.gov/newsroom/releases/eta/eta20250630)

200. Keely Quinlan, "Industry groups 'alarmed' Education Department cuts may weaken school cybersecurity," *StateScoop*, March 14, 2025. (https://statescoop.com/industry-groups-alarmed-education-department-cuts-may-weaken-school-cybersecurity); U.S. Executive Order 14199, "Withdrawing the United States From and Ending Funding to Certain United Nations Organizations and Reviewing United States Support to All International Organizations," February 4, 2025. (https://www.whitehouse.gov/presidential-actions/2025/02/withdrawing-the-united-states-from-and-ending-funding-to-certain-united-nations-organizations-and-reviewing-united-states-support-to-all-international-organizations)

201. Anna Prothero and Lauraine Langreo, "How Will Trump Budget Cuts Affect School Cybersecurity?" *GovTech*, April 7, 2025. (https://www.govtech.com/education/k-12/how-will-trump-budget-cuts-affect-school-cybersecurity)

202. Center for International Security, "2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience," March 6, 2025. (https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report)

203. Consortium for School Networking, "School District Petition to Restore Federal Leadership on K-12 Cybersecurity and Educational Technology," July 15, 2025, pages 1-2. (https://www.cosn.org/wp-content/uploads/2025/07/CoSN-School-District-Cybersecurity-Petition-.pdf)

204. 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://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf)

205. Christian Vasquez, "Newmark initiative will bring online a network of civil defense hackers," *CyberScoop*, September 18, 2024. (https://cyberscoop.com/berkeley-volunteer-network-civil-cyber); The Consortium of Cybersecurity Clinics, "Cybersecurity for the public good," accessed August 20, 2025. (https://cybersecurityclinics.org); Brandi Vesco, "Arizona High Schools to Launch Cybersecurity Clinics," *GovTech*, March 24, 2025. (https://www.govtech.com/education/k-12/arizona-high-schools-to-launch-cybersecurity-clinics); Google, "Investing in America's cybersecurity workforce," accessed August 20, 2025. (https://cyberclinics.withgoogle.com)

206. U.S. Office of Personnel Management, "Extension and Amendment of the Government-wide Direct Hire Appointing Authority for Scientific, Technical, Engineering and Mathematics (STEM) Positions, Acquisitions, and Cybersecurity and Related Positions," September 23, 2024, page 1. (https://chcoc.gov/content/extension-and-amendment-government-wide-direct-hire-appointing-authority-scientific)

207. The White House, "Hiring Freeze," January 20, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/hiring-freeze); The White House, "Ensuring Accountability and Prioritizing Public Safety in Federal Hiring," July 7, 2025. (https://www.whitehouse.gov/presidential-actions/2025/07/ensuring-accountability-and-prioritizing-public-safety-in-federal-hiring)

208. Sam Sabin, "Exclusive: One-third of top U.S. cyber force has left since Trump took office," *Axios*, June 3, 2025. (https://www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts)

209. Lydia DePillis, "Why 'Probationary' Employees Are a Target in Federal Job Cuts," *The New York Times*, February 25, 2025. (https://www.nytimes.com/2025/02/25/business/economy/probationary-federal-workers-trump-cuts.html); Madeleine Ngo, "Trump's Cuts to Federal Work Force Push Out Young Employees," The New York Times, March 6, 2025. (https://www.nytimes.com/2025/03/06/us/politics/trump-cuts-young-federal-workers.html)

210. Christine Mui, "CHIPS employees fired at NIST," *Politico*, March 3, 2025. (https://subscriber.politicopro.com/article/2025/03/chips-employees-fired-at-nist-00209461)

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

212. Justin Doubleday, "DHS cancels federal neurodiversity workforce contract," *Federal News Network*, April 15, 2025. (https://federalnewsnetwork.com/hiring-retention/2025/04/dhs-cancels-federal-neurodiversity-workforce-contract)

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

214. U.S. Executive Order 14151, "Ending Radical and Wasteful Government DEI Programs and Preferencing," January 20, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/ending-radical-and-wasteful-government-dei-programs-and-preferencing); U.S. Executive Order 14173, "Ending Illegal Discrimination and Restoring Merit-Based Opportunity," January 21, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/ending-illegal-discrimination-and-restoring-merit-based-opportunity); U.S. Office of Personnel Management, "Guidance Regarding RIFs of DEIA Offices," January 24, 2025. (https://www.opm.gov/media/0gpnja24/opm-memo-guidance-regarding-rifs-of-deia-offices-1-24-2025.pdf)

215. Dana Nickel, "DEI and the cyber workforce," *Politico*, March 24, 2025. (https://www.politico.com/newsletters/weekly-cybersecurity/2025/03/24/cyber-experts-weigh-in-on-dei-rollbacks-00244343); Leadership Bainery, "HBCUs Are Doing The Work—Without The Wallet," *Forbes*, August 4, 2025. (https://www.forbes.com/sites/forbeseq/2025/08/04/hbcus-are-doing-the-work-without-the-wallet)

216. U.S. House of Representatives, Homeland Security Committee, "Committee Advances 'Cyber PIVOTT Act, Adopts 119th Congress Oversight Plan," February 26, 2025. (https://homeland.house.gov/2025/02/26/committee-advances-cyber-pivott-act-adopts-119th-congress-oversight-plan)

217. Weslan Hansen, "Democrats Abandon Cyber PIVOTT Bill, Citing Federal Layoffs," *MeriTalk*, February 26, 2025. (https://www.meritalk.com/articles/democrats-abandon-cyber-pivott-bill-citing-federal-layoffs)

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

219. Terry Gerton, "We have the defense industrial base we contracted for a generation ago. Can it meet today's demands?" *Federal News Network*, August 18, 2025. (https://federalnewsnetwork.com/defense-industry/2025/08/we-have-the-defense-industrial-base-we-contracted-for-a-generation-ago-can-it-meet-todays-demands); U.S. Government Accountability Office, "Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers," July 24, 2025. (https://www.gao.gov/products/gao-25-107283)

220. U.S. Department of Homeland Security and 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 Supply Chain Report_2.pdf); U.S. National Science Foundation, Press Release, "NSF advances 29 semifinalists in the second NSF Regional Innovation Engines competition," July 8, 2025. (https://www.nsf.gov/news/nsf-advances-29-semifinalists-second-nsf-regional-innovation)

221. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1642. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf#page=278); U.S. National Science Foundation, "Find Potential NSF Engines," accessed August 15, 2024. (https://new.nsf.gov/funding/initiatives/regional-innovation-engines/find-potential-nsf-engines); U.S. National Science Foundation, Press Release, "NSF advances 29 semifinalists in the second NSF Regional Innovation Engines competition," July 8, 2025. (https://www.nsf.gov/news/nsf-advances-29-semifinalists-second-nsf-regional-innovation)

222. U.S. Department of Commerce, Office of Public Affairs, Press Release, "Tech Hubs Program Fact Sheet," May 16, 2025. (https://www.commerce.gov/news/fact-sheets/2025/05/tech-hubs-program-fact-sheet)

223. U.S. National Science Foundation, "NSF Engines Portfolio," accessed August 16, 2025. (https://www.nsf.gov/funding/initiatives/regional-innovation-engines/portfolio); U.S. National Science Foundation, "About NSF Engines," accessed August 16, 2025. (https://www.nsf.gov/funding/initiatives/regional-innovation-engines/about-nsf-engines); U.S. National Science Foundation, Press Release, "NSF advances 29 semifinalists in the second NSF Regional Innovation Engines competition," July 8, 2025. (https://www.nsf.gov/news/nsf-advances-29-semifinalists-second-nsf-regional-innovation)

224. U.S. Semiconductor Industry Association, "America's Chip Resurgence: Over $630 Billion in Semiconductor Supply Chain Investments," July 28, 2025. (https://www.semiconductors.org/chips-incentives-awards)

225. David Sacks and Adam Segal, "Unpacking TSMC's $100 Billion Investment in the United States," *Council on Foreign Relations*, March 4, 2025. (https://www.cfr.org/blog/unpacking-tsmcs-100-billion-investment-united-states)

226. John Ruwitch, "Trump says Nvidia will hand the U.S. 15% of its H20 chip sales to China," *NPR*, August 11, 2025. (https://www.npr.org/2025/08/11/nx-s1-5498689/trump-nvidia-h20-chip-sales-china); Kathryn Watson, "Conservatives and economists warn Trump admin. Against buying stakes in U.S. companies beyond Intel," *CBS News*, August 29, 2025. (https://www.cbsnews.com/news/trump-intel-stake-consertatives-economists-response)

227. U.S. Department of Defense, Press Release, "Department of Defense and U.S. Small Business Administration Announce First Licensed and Green Light Approved Funds for the Small Business Investment Company Critical Technology Initiative," October 22, 2024. (https://www.defense.gov/News/Releases/Release/Article/3942474/department-of-defense-and-us-small-business-administration-announce-first-licen); U.S. Department of Defense, "DoD Critical Technology Areas," accessed August 18, 2025. (https://www.cto.mil/osc/critical-technologies)

228. U.S. Department of Defense, Press Release, "Department of Defense and U.S. Small Business Administration Publish Names of First 18 Licensed and Green Light Approved Funds for the Small Business Investment Company Critical Technologies Initiative," January 17, 2025. (https://www.defense.gov/News/Releases/Release/Article/4032999/department-of-defense-and-us-small-business-administration-publish-names-of-fir)

229. 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)

230. National Defense Authorization Act of 2020, P.L. 116-92, 133 STAT. 2188. (https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf#page=992)

231. Office of the Director of National Intelligence, the National Counterintelligence and Security Center, "Supply Chain Risk Management," accessed August 18, 2025. (https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats)

232. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf#page=960)

233. 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)

234. U.S. Department of Homeland Security, Press Release, "Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security," November 14, 2024. (https://www.dhs.gov/archive/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure) U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "CISA and Partners Release Asset Inventory Guidance to Strengthen Operational Technology Security," August 13, 2025. (https://www.cisa.gov/news-events/news/cisa-and-partners-release-asset-inventory-guidance-strengthen-operational-technology-security); U.S. Department of Homeland Security, Science and Technology Directorate, Press Release, "News Release: DHS S&T Releases Best Practices for Supporting Critical Infrastructure," February 25, 2025. (https://www.dhs.gov/science-and-technology/news/2025/02/25/dhs-st-releases-best-practices-supporting-critical-infrastructure); U.S. Department of Defense, Office of the Director, Developmental Test, Evaluation, and Assessments, and Office of the Under Secretary of Defense for Research and Engineering, "Department of Defense Cyber Developmental Test and Evaluation Guidebook Version 3.0," June 27, 2025. (https://aaf.dau.edu/storage/2025/06/Cyber-DTE-Guidebook-V3-June2025_Final.pdf)

235. Ethan Huffman, "TAIGR: Testing the limits of AI on the power grid," *Idaho National Laboratory*, August 11, 2025. (https://inl.gov/feature-story/taigr-testing-the-limits-of-ai-on-the-power-grid)

236. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, P.L. 118-159, 138 Stat. 2450. (https://www.congress.gov/118/plaws/publ159/PLAW-118publ159.pdf#page=678); Competitive Bidding Rules for Auction of AWS-3 Licenses, Federal Communications Commission, 90 Federal Register 36385, August 4, 2025. (https://www.federalregister.gov/documents/2025/08/04/2025-14725/competitive-bidding-rules-for-auction-of-aws-3-licenses)

237. Federal Communications Commission, "Report And Order And Further Notice Of Proposed Rulemaking," May 27, 2025, page 2. (https://docs.fcc.gov/public/attachments/FCC-25-27A1.pdf)

238. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, P.L. 118-159, 138 Stat. 2450. (https://www.congress.gov/118/plaws/publ159/PLAW-118publ159.pdf#page=678)

239. U.S. Government Accountability Office, "Priority Open Recommendations: National Telecommunications and Information Administration," July 14, 2025. (https://www.gao.gov/products/gao-25-108178)

240. U.S. Department of Commerce, National Institute of Standards and Technology, Press Release, "NIST Awards $15 Million to ASTM International to Establish Standardization Center of Excellence," October 14, 2024. (https://www.nist.gov/news-events/news/2024/10/nist-awards-15-million-astm-international-establish-standardization-center)

241. U.S. Department of State, Press Release, "Implementing the President's Executive Order on Reevaluating and Realigning United States Foreign Aid," January 26, 2025. (https://www.state.gov/implementing-the-presidents-executive-order-on-reevaluating-and-realigning-united-states-foreign-aid)

242. The White House, Council on Supply Chain Resilience, "2021–2024 Quadrennial Supply Chain Review," December 19, 2024, page 92. (https://www.trade.gov/sites/default/files/2025-01/20212024-Quadrennial-Supply-Chain-Review.pdf); U.S. Trade Development Agency, "USTR Finalizes Action on China Tariffs Following Statutory Four-Year Review," September 13, 2024. (https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/september/ustr-finalizes-action-china-tariffs-following-statutory-four-year-review); U.S. Trade Development Agency, Press Release, "USTR Section 301 Action on China's Targeting of the Maritime, Logistics, and Shipbuilding Sectors for Dominance," April 17, 2025. (https://ustr.gov/about/policy-offices/press-office/press-releases/2025/april/ustr-section-301-action-chinas-targeting-maritime-logistics-and-shipbuilding-sectors-dominance)

243. Export-Import Bank, Press Release, "Export-Import Bank of the United States Board of Directors Approves Supply Chain Resiliency Initiative to Protect U.S. Jobs and Shift Critical Mineral Supply Chains Back to the United States and Away from the People's Republic of China," January 8, 2025. (https://www.exim.gov/news/export-import-bank-united-states-board-directors-approves-supply-chain-resiliency)

244. Rep. Young Kim, "Reauthorizing the U.S. Development Finance Corporation," *Opening Statement before the House Committee on Foreign Affairs*, March 11, 2025, page 4. (https://www.congress.gov/119/chrg/CHRG-119hhrg60302/CHRG-119hhrg60302.pdf)

245. The White House, "Fact Sheet: President Donald J. Trump Encourages Foreign Investment While Protecting National Security," February 21, 2025. (https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-encourages-foreign-investment-while-protecting-national-security)

246. "Division H - Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2023," *U.S. Senate Document Depository*, July 5, 2022, page 236. (https://www.appropriations.senate.gov/imo/media/doc/Division H - LHHS Statement FY23.pdf); Senate Appropriations Committee, "Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Bill, 2025, Report," August 1, 2024, page 265. (https://www.congress.gov/118/crpt/srpt207/CRPT-118srpt207.pdf#page=265); iCivics, Press Release, "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); Senate Appropriations Committee, "Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2026, Report," July 31, 2025, page 284. (https://www.appropriations.senate.gov/imo/media/doc/fy26_lhhs_senate_report.pdf#page=284)

247. iCivics, "Americans From All Backgrounds Will Make The Case For Civic Education During Civic Learning Week, March 10-14, 2025," March 7, 2025. (https://www.prnewswire.com/news-releases/americans-from-all-backgrounds-will-make-the-case-for-civic-education-during-civic-learning-week-march-1014-2025-302395581.html); Center for Revitalizing American Institutions and Working Group on Civics and American Citizenship Research Teams, "Civic Learning Week National Forum: Celebrating Many Voices, One Nation," *Hoover Institution*, April 14, 2025. (https://www.hoover.org/news/civic-learning-week-national-forum-celebrating-many-voices-one-nation); Tani Cantil-Sakauye and Mark Baldassare, "Californians and Civic Education," *Public Policy Institute of California*, June 23, 2025. (https://www.ppic.org/publication/californians-and-civic-education); Penne Soltysik, "Power of Democracy and iCivics Partner for Summer School for Teachers," *California Courts NewsRoom*, July 24, 2025. (https://newsroom.courts.ca.gov/news/power-democracy-and-icivics-partner-summer-school-teachers)

248. Gabe Kaminsky and Madeleine Rowley, "Joe Biden Made More Than 600 Grants to Stop 'Disinformation.' Donald Trump Now Has a Plan for Them," *The Free Press*, April 16, 2025. (https://www.thefp.com/p/joe-biden-made-600-grants-to-stop-disinformation-misinformation-donald-trump-cancels-awards)

249. U.S. Executive Order 14149, "Restoring Freedom of Speech and Ending Federal Censorship," January 20, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship)

250. Reporters Without Borders, "USA: Trump's foreign aid freeze throws journalism around the world into chaos," June 2, 2025. (https://rsf.org/en/usa-trump-s-foreign-aid-freeze-throws-journalism-around-world-chaos)

251. U.S. Executive Order 14159, "Protecting The American People Against Invasion," January 20, 2025. (https://www.whitehouse.gov/presidential-actions/2025/01/protecting-the-american-people-against-invasion)

252. Steven Lee Meyers, "Trump Administration Cancels Scores of Grants to Study Online Misinformation," *The New York Times*, May 15, 2025. (https://www.nytimes.com/2025/05/15/business/trump-online-misinformation-grants.html)

253. Ali Swenson and Christina A. Cassidy, "Dismantling of federal efforts to monitor election interference creates opening for foreign meddling," *Associated Press*, February 16, 2025. (https://apnews.com/article/trump-election-security-fbi-cisa-foreign-interference-98f1e17c8a6d5923db945a27f06458e7)

254. Tom Spring, "At RSAC, Kristi Noem calls to rein in CISA and reset DHS cyber strategy," *SC Media*, April 30, 2025. (https://www.scworld.com/news/at-rsac-kristi-noem-calls-to-rein-in-cisa-and-reset-dhs-cyber-strategy)

255. Steven Lee Meyers, Julian E. Barnes, and Sheera Frenkel, "Trump Dismantles Government Fight Against Foreign Influence Operations," *The New York Times*, February 20, 2025. (https://www.nytimes.com/2025/02/20/business/trump-foreign-influence-election-interference.html)

256. Secretary of State Marco Rubio, "Rubio: To Protect Free Speech, The Censorship-Industrial Complex Must Be Dismantled," *The Federalist*, April 16, 2025. (https://thefederalist.com/2025/04/16/rubio-to-protect-free-speech-the-censorship-industrial-complex-must-be-dismantled)

257. Colin Wood, "Federal cuts to information-sharing groups may damage nation's security posture, warn officials," *StateScoop*, March 13, 2025. (https://statescoop.com/eiisac-msisac-center-internet-security-cisa-cuts-2025)

258. According to the Brennan Center for Justice, 858 local election officials responded to their 2025 survey conducted between April 15 and May 17, 2025. Survey invitations were emailed to a list of 8,491 local election officials compiled with assistance from the U.S. Vote Foundation. Brennan Center for Justice, "Local Election Officials Survey — July 2025," July 10, 2025. (https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-july-2025); Brennan Center for Justice, "Local Election Officials Survey 2025," July 10, 2025, page 1; (https://www.brennancenter.org/media/14129/download/2025_local_election_officials_6.25_export072925.pdf?inline=1); Colin Wood, "Federal cuts to information-sharing groups may damage nation's security posture, warn officials," *StateScoop*, March 13, 2025. (https://statescoop.com/eiisac-msisac-center-internet-security-cisa-cuts-2025)

259. David Klepper, "Disinformation and conspiracy theories cloud Helene recovery efforts in hard-hit areas," *Public Broadcasting Service*, October 5, 2024. (https://www.pbs.org/newshour/nation/disinformation-and-conspiracy-theories-cloud-helene-recovery-efforts-in-hard-hit-areas); Shada Udvardy, "The Terrible Texas Flood Tragedy Made Worse by Trump Administration's Dysfunctional FEMA Response," *Union of Concerned Scientists*, July 17, 2025. (https://blog.ucs.org/shana-udvardy/the-terrible-texas-flood-tragedy-made-worse-by-trump-administrations-dysfunctional-fema-response)

260. U.S. Department of Justice, Office of the Attorney General, "General Policy Regarding Charging, Plea Negotiations, and Sentencing," February 5, 2025, page 4. (https://www.justice.gov/ag/media/1388541/dl)

261. Ki Hong, Charles Ricciardelli, and Alexa Santry, "Navigating the Foreign Agents Registration Act's shifting sands: what to make of DOJ's new enforcement priorities," *Reuters*, April 1, 2025. (https://www.reuters.com/legal/legalindustry/navigating-foreign-agents-registration-acts-shifting-sands-what-make-dojs-new-2025-04-01)

262. Amending and Clarifying Foreign Agents Registration Act Regulations, Office of the Attorney General, Department of Justice, 90 Federal Register 40, January 2, 2025. (https://www.federalregister.gov/documents/2025/01/02/2024-30871/amending-and-clarifying-foreign-agents-registration-act-regulations)

263. Clare Y. Cho and Ling Zhu, "Social Media: Dissemination and Moderation Practices," *Congressional Research Services*, updated March 20, 2025, page 1. (https://www.congress.gov/crs_external_products/R/PDF/R46662/R46662.11.pdf)

264. *TikTok Inc. v. Garland*, 604 U.S. ___ (2025). (https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf); *TikTok Inc. and ByteDance Ltd. v. Garland*, 122 F.4th 930 (D.C. Cir. 2024). (https://law.justia.com/cases/federal/appellate-courts/cadc/24-1113/24-1113-2024-12-06.html)

265. The Editorial Board, "Trump Is Letting TikTok (and China) Win," *The New York Times*, August 8, 2025. (https://www.nytimes.com/2025/08/08/opinion/trump-tiktok-ban-china-congress.html)

266. Federal Trade Commission, Press Release, "Federal Trade Commission Launches Inquiry on Tech Censorship," February 20, 2025. (https://www.ftc.gov/news-events/news/press-releases/2025/02/federal-trade-commission-launches-inquiry-tech-censorship)

About the Authors

Jiwon Ma is a senior policy analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. Her research focuses on the cyber threat landscape and adversarial strategies and capabilities, emerging technologies, cyber deterrence, and U.S. cyber and international security policies. She is the lead author of CSC 2.0's annual assessment of the implementation of Cyberspace Solarium Commission recommendations. Jiwon received a master's degree in international affairs from Columbia University's School of International and Public Affairs and a BA in global studies and education from Lesley University.

ACKNOWLEDGEMENTS

The authors of the CSC 2.0 Annual Assessment report would like to express their gratitude to 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 are especially grateful to Annie Fixler, whose steady leadership and editorial discipline have shaped not only this year's assessment but also the three that preceded it. Her guidance has been essential in ensuring each publication's clarity, coherence, and timeliness. We also thank David Adesnik, together with editors Jason Fields, David May, and Grant Wishard, for their sharp eyes and skillful refinements throughout the drafting process. We are likewise indebted to Katy Wickberg and Allie Shisgal for their coordination of logistics, which made the release of this report possible. While many experts helped refine the assessment, any errors in fact or judgment are ours alone. Finally, we extend our thanks to Danny Ackerman and Pavak Patel for transforming complex analysis into compelling visualizations and designs that have animated each of the CSC 2.0 Annual Assessments.

Cover Photo: Senator Angus King 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

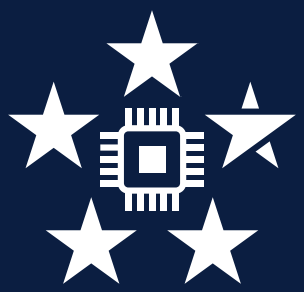
Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

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