CSC 2.0

September 2023

2023 Annual Report on Implementation

Jiwon Ma
RADM (Ret.) Mark Montgomery

Table of Contents

Executive Summary **1**

Evaluating Progress **3**

Recommendations From the March 2020 CSC Report **4**

Pillar 1: Reform the U.S. Government's Structure and Organization for Cyberspace 4

Pillar 2: Strengthen Norms and Non-military Tools 6

Pillar 3: Promote National Resilience 8

Pillar 4: Reshape the Cyber Ecosystem Toward Greater Security 11

Pillar 5: Operationalize Cybersecurity Collaboration With the Private Sector 15

Pillar 6: Preserve and Employ the Military Instrument of Power 17

CSC White Papers **19**

White Paper #1: Cybersecurity Lessons From the Pandemic 19

White Paper #2: National Cyber Director 20

White Paper #3: Growing a Stronger Federal Cyber Workforce 21

White Paper #4: Building a Trusted ICT Supply Chain 23

White Paper #6: Countering Disinformation in the United States 25

Conclusion **26**

Executive Summary

In the three years since the publication of the Cyberspace Solarium Commission's (CSC's) March 2020 report, both the executive and legislative branches have taken significant steps to improve the government and the nation's cybersecurity. In fact, nearly 70 percent of the recommendations in the initial CSC report have been implemented or are nearing implementation. But America's cyber adversaries have been busy in the intervening three years. Russia and China have conducted significant espionage attacks on the U.S. government and industries and have reportedly embedded malware in U.S. critical infrastructure to facilitate future nefarious activity. Criminal actors have also expanded both ransomware and cyber theft activities. We cannot afford to pause in the pursuit of enhanced cybersecurity.

Lawmakers have remained industrious on cybersecurity issues, both authorizing more cybersecurity programs and ensuring these initiatives have the resources critical to their success. At the end of last year, for example, Congress codified the new State Department's Bureau of Cyberspace and Digital Policy, which will promote responsible state conduct in cyberspace and advance U.S. interests. Congress has also increased funding for the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security from $2 billion for fiscal year (FY) 2020[1] to $2.9 billion for FY23,[2] a 45 percent increase. Further growth is expected in FY24.[3] The nation will reap the benefits of these cybersecurity investments for years to come.

The executive branch has made productive changes. The Office of the National Cyber Director (ONCD) — having reached full operating capacity — issued a comprehensive National Cyber Strategy and associated implementation plan as well as the first-ever National Cybersecurity Workforce and Education Strategy. CISA has continued to improve its technical support to other federal agencies, establish cyber performance goals, and develop plans, sharing, and response efforts through the Joint Cyber Defense Collaborative. The Securities and Exchange Commission issued new rules to increase corporate responsibility for cybersecurity. The National Security Council has coordinated responses to an ever-increasing number of international espionage and malicious cyber incidents, while the National Security Agency has expanded and improved its information sharing and support efforts with targeted industry partners. Despite these efforts, federal agencies have an uneven record of collaboration with the private sector, although the Defense and Energy departments have made more progress than others.

Collaboration with the private sector is indispensable since deterring cyber threats depends on the resilience of the U.S. economy and the critical infrastructure that supports it, so the federal government cannot handle the job alone. Significant work remains necessary to build an effective cybersecurity partnership between the public and private sectors. This will require a careful balancing of incentivization, collaboration, and, only where necessary, regulation across and between each of the country's critical infrastructure sectors. A similar effort is needed to enhance cooperation with like-minded international allies and partners, ensuring a resilient global economy.

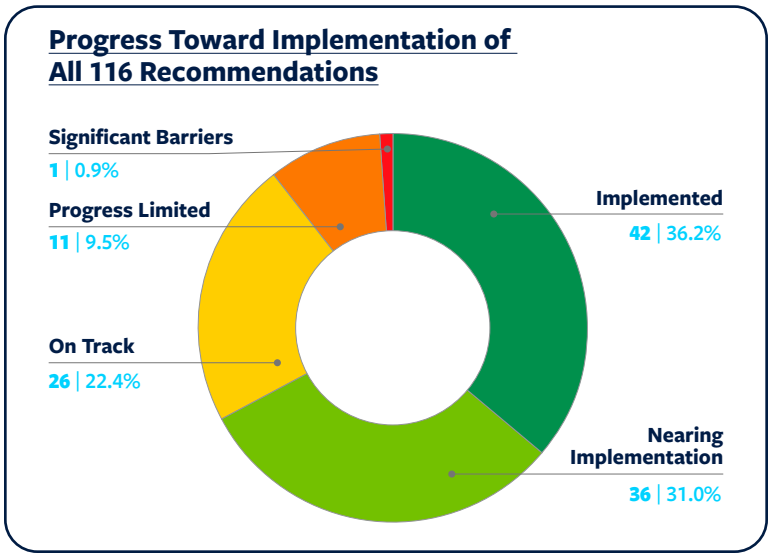
To support these efforts, the U.S. government must continue to empower existing cybersecurity agencies and invest in hardening its security posture. As part of this effort, the government should continue implementing the recommendations of the CSC. Congress created this commission to identify a strategic approach to securing cyberspace. Over the course of three years, the commission developed 116 recommendations, many of which are accompanied by model legislative language. Nearly 70 percent of these recommendations have been fully implemented or are nearing implementation, and an additional 20 percent are on track to be implemented.

This assessment details progress toward implementing the commission's original work, consisting of its report and white papers. The assessment also suggests actions that can be taken to accomplish more recommendations. We urge readers to consider this report as a way to gauge America's collective efforts, allowing many government and industry stakeholders to identify areas suitable for building or deepening partnerships to achieve the broader objective of protecting our national cybersecurity.

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

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

Timeline



September 2022

- The Senate confirms Nathaniel Fick as the inaugural ambassador at large for cyberspace and digital policy at the State Department.
- The president issues an executive order expanding the factors considered by the Committee on Foreign Investment in the United States to include cybersecurity.

December 2022

- The Cyber National Mission Force becomes a subordinate unified command of U.S. Cyber Command, further reflecting its operational success.
- As part of the FY23 National Defense Authorization Act, Congress establishes the Bureau of Cyberspace and Digital Policy through the passage of the Cyber Diplomacy Act and authorizes the Federal Risk and Authorization Management Program to standardize security assessment of cloud computing products and services used for unclassified federal information.
- The FY23 omnibus spending bill authorizes over $2 billion in funding for CISA to carry out its responsibilities and $22 million for the Office of the National Cyber Director to fully staff its office.
- The Office of the National Cyber Director establishes the National Cyber Workforce Coordination Group, an interagency forum to address federal workforce and education challenges.

March 2023

- The White House issues the National Cybersecurity Strategy, serving as the declaratory policy for U.S. cybersecurity policies.

April 2023

- Ambassador Fick announces that the Bureau of Cyberspace and Digital Policy is on track to place a cyber and digital officer in all U.S. embassies by the end of 2024.

May 2023

- The Department of Defense releases an unclassified summary of its cyber strategy.

July 2023

- The White House issues the National Cybersecurity Strategy Implementation Plan, a roadmap to execute the National Cybersecurity Strategy.
- The White House announces the U.S. Cyber Trust Mark program to create a voluntary cybersecurity labeling program for Internet of Things consumer devices.
- The U.S. Securities and Exchange Commission adopts rules for companies to disclose material cybersecurity incidents and cyber risk management practices to increase transparency and public awareness of systemic risks.
- The White House issues the National Cyber Workforce and Education Strategy.

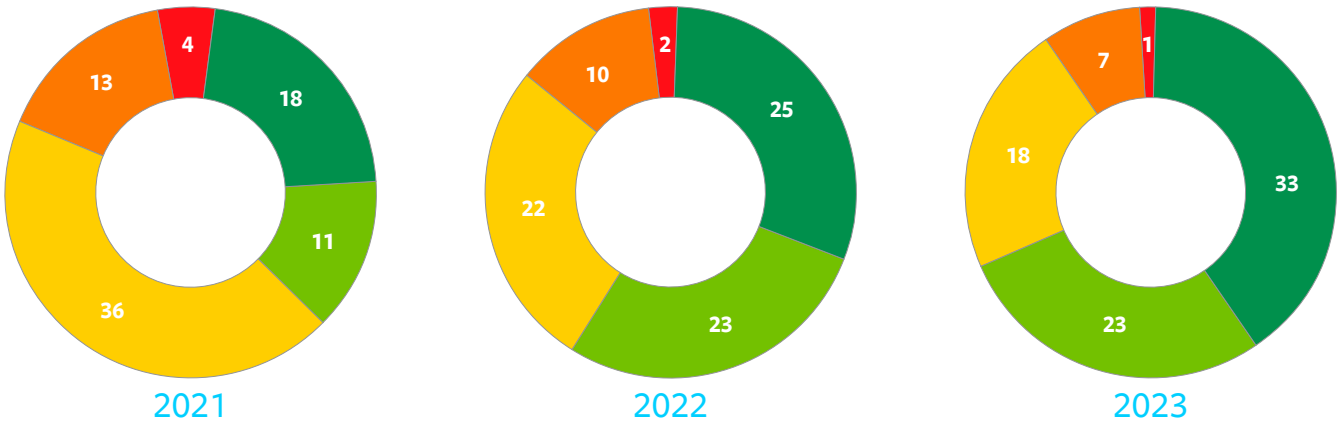
August 2023

- The White House announces new initiatives aimed at bolstering cybersecurity in K-12 schools across America.

Evaluating Progress

The fiscal year 2021 National Defense Authorization Act (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.[4] This report is the third annual implementation review responding to that mandate. While work is still required to fully implement all of the CSC's recommendations, a review of progress shows that cybersecurity leaders throughout the government continue to take significant steps forward.

Progress Toward Implementation of the March 2020 Recommendations (Number of Recommendations in Each Category, by Year)



This report documents progress and identifies future actions required to advance the CSC's 116 recommendations along the path toward protecting the United States from cyberattacks of significant consequence. Indicators of progress toward implementation of commission recommendations are varied but appear most frequently in authorizing legislation, appropriations, and executive branch policy and actions. This progress is given a single rating for each recommendation, as indicated by the following color-coding system:

Implementation Status	
	Implemented: Legislation has been passed, an executive order issued, or other definitive action taken.
	Nearing Implementation/Partial Implementation: The recommendation is included in legislation or an executive order that has a clear path to approval, or it is partially implemented in law/policy.
	On Track: The recommendation is being considered for a legislative vehicle, an executive order or other policy is being considered, or there are measurable/reported signs of progress.
	Progress Limited/Delayed: The recommendation has not been rejected, but it is not in a legislative vehicle, and there are no known policy actions underway.
	Significant Barriers to Implementation: These recommendations are not expected to move in the immediate future but are ready to be taken up if future crises spur action.

Recommendations From the March 2020 CSC Report

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

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

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

1.1 – Issue an Updated National Cyber Strategy: *Implemented via executive action.* On March 2, 2023, the Biden administration issued the National Cybersecurity Strategy.[5] The Office of the National Cyber Director led the drafting of the strategy with input from cybersecurity experts inside and outside of government. The strategy includes five pillars: defend critical infrastructure; disrupt and dismantle threat actors; shape market forces to drive security and resilience; invest in a resilient future; and forge international partnerships to pursue shared goals.[6] The administration then issued a "roadmap" for executing the strategy,[7] detailing 65 initiatives led by 18 departments and agencies over the next three fiscal years.[8] Acting National Cyber Director (NCD) Kemba Walden called the National Cybersecurity Strategy Implementation Plan a "living document," anticipating adjustments to the plan "in response to changing cyber threat landscape."[9]

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

1.1.2 – Promulgate a New Declaratory Policy: *Implemented via executive action and legislation*. As noted in previous recommendations, the publication of the National Cybersecurity Strategy serves as a declaratory policy vital for deterrence against adversaries of the United States, and its allies and partners. The strategy notes that Washington "will use all instruments of national power"[10] to respond to malicious cyber actors. The strategy publicly declares that, working with allies and partners, the United States will impose cyber and/or non-cyber costs on adversaries, including for cyber activity that falls "below the threshold of armed conflict."[11] In addition, last year, Congress authorized the president to use U.S. Cyber Command to respond if the government determines that "there is an active, systematic, and ongoing campaign of attacks in cyberspace by a foreign power against the Government or the critical infrastructure."[12] This declaratory policy supports the intent of this recommendation.

1.2 – Create House Permanent Select and Senate Select Committees on Cybersecurity: *Faces significant barriers to implementation.* Significant pushback against this recommendation continued for a third year. Prior to the end of the commission's tenure, staff drafted legislative language should a future emergency create the political impetus to overcome existing barriers.

1.2.1 – Re-establish the Office of Technology Assessment: *On track via appropriated funding.* In FY21 and FY22 appropriations, Congress indicated that it prefers to increase funding for the Government Accountability Office (GAO) and the Congressional Research Service (CRS) over re-establishing the Office of Technology Assessment.[13] The GAO's FY24 budget request to Congress notes that funding increases will allow the office to "maximize... science and technology reporting capabilities."[14] The CRS's FY24 budget also requests a $13 million increase over FY23 enacted levels, a nearly 10 percent increase.[15] These budget increases may suffice to fill the gap left by the loss of the Office of Technology Assessment.

1.3 – Establish a National Cyber Director Position: *Implemented via executive action; further legislative action required.* After serving 17 months as the inaugural cyber advisor to the president, NCD Chris Inglis announced his departure from the position in February 2023. Despite letters from the commission co-chairs, other members of Congress, and private industry urging the swift nomination of a replacement,[16] the administration did not announce the nomination of Harry Coker, Jr. as the next NCD until July.[17] In the interim, Kemba Walden, the principal deputy NCD, has served admirably as acting director. Should the absence of a Senate-confirmed NCD persist, this recommendation would be considered only partially implemented.

1.4 – Strengthen the Cybersecurity and Infrastructure Security Agency: *Implemented via legislative action but further action also required; funds appropriated*. Congress has continued to equip CISA with appropriate funding and resources to carry out its responsibilities. The FY23 omnibus spending bill included $2.097 billion for CISA, which is $313 million above the FY22 enacted amount, or a 12 percent increase.[18] At the annual DEFCON conference this year, CISA Director Jen Easterly noted that she has the authorities she needs thanks to the CSC.[19] In terms of resources, Congress has consistently provided CISA with the increased appropriations it needs to be successful. A provision to establish a five-year term for the CISA director, however, has failed to pass Congress despite its inclusion in the House version of the FY23 NDAA.[20] Additionally, legislation to codify CISA as the national risk management agency has also faced hurdles to implementation but has been attempted in both 2022 and 2023.

1.4.1 – Codify and Strengthen the Cyber Threat Intelligence Integration Center: *Nearing implementation/partial implementation; further legislative action and appropriations required.* As noted in last year's assessment, the Biden administration re-established the Cyber Threat Intelligence Integration Center (CTIIC) at the Office of the Director of National Intelligence. The National Cybersecurity Strategy calls upon sector risk management agencies to work with CTIIC, CISA, and law enforcement agencies to "identify intelligence needs and priorities within their sectors."[21] The Intelligence Authorization Act, passed as part of the FY22 spending omnibus, calls for a "report on the potential to strengthen all-source intelligence integration relating to foreign cyber threats."[22] Full implementation of this recommendation will require action in response to the mandated report.

1.4.2 – Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force: *Implemented via increased appropriations.* The FY24 president's budget includes an additional $63 million to "build cyber investigative capabilities at FBI field divisions nationwide."[23] Additionally, the FBI requested four full-time positions and $27.2 million to enhance its cybersecurity posture and internal networks.[24]

1.5 – Diversify and Strengthen the Federal Cyberspace Workforce: *Implemented via legislative actions and increased appropriations*. Cybersecurity programs face recurring budgetary constraints, but there were various opportunities for increased funding in FY23. The passage of the CHIPS and Science Act last year provided increased resources for the federal cyber workforce programs.[25] In March, the Office of Personnel Management published implementation guidance on the Federal Rotational Cyber Workforce Program,[26] which allows federal employees to gain exposure to different cybersecurity and IT-related job functions through rotations to other federal agencies.[27] Meanwhile, on Capitol Hill, the Senate Homeland Security and Governmental Affairs Committee passed the Federal Cybersecurity Workforce Expansion Act out of committee in July.[28] If signed into law, the legislation would create a cybersecurity-focused upskilling pilot program at the Department of Veterans Affairs for service members transitioning to civilian life and a cybersecurity apprenticeship program within CISA.[29] Most significantly, the Office of the National Cyber Director published the National Cyber Workforce and Education Strategy

with four core tenets focused on awareness, education, and the national and federal workforces.[30] In light of these actions, this recommendation is considered fully implemented, but cybersecurity workforce development must be a long-term effort that continues far past the specific recommendations made here.

1.5.1 – Improve Cyber-Oriented Education: *Implemented via increased appropriations.* The president's budget request for FY23 reallocated CISA's budget for K-12 cybersecurity education efforts to the National Science Foundation.[31] This move would have greatly undermined the ongoing efforts of CISA and overburdened the foundation's work. However, in the FY23 omnibus appropriations bill, Congress increased CISA funding to $6.8 million for investments in K-12 cybersecurity programs, including the Cybersecurity Training and Education Assistance Program (CETAP).[32] The president's FY24 budget request reversed course, affirming CISA's role. While the recommendation is deemed fully implemented, the administration and Congress must maintain consistent funding for cybersecurity education and training programs.

Pillar 2: Strengthen Norms and Non-military Tools

Strengthen Norms and Non-military Tools				
Rec. Number	Recommendation Title	2021	2022	2023
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: *Implemented via executive and legislative action*. In September 2022, the Senate confirmed Nathaniel Fick as the first-ever ambassador-at-large for cyber, leading the Department of State's Bureau of Cyberspace and Digital Policy (CDP).[33] Meanwhile, Congress also permanently established the bureau with the passage of the Cyber Diplomacy Act as part of the FY23 NDAA. In addition to listing the duties of the bureau, the statute also provides the secretary of state with special hiring authorities, which allows CDP to appoint "up to 25 employees to cyber positions."[34] This summer, Ambassador Fick said that the CDP is on track to place a cyber and digital officer in all U.S. embassies by the end of 2024.[35] In total, the FY24 budget submission to Congress requests $22.1 million for CDP, an increase of $1.4 million above the FY23 adjusted enacted level.[36] While this recommendation is considered fully implemented, the success of the new bureau will require consistent appropriations and leadership to further cyber diplomacy and capacity building efforts.

2.1.1 – Strengthen Norms of Responsible State Behavior in Cyberspace: *Implemented via executive action.* Pillar five of the National Cybersecurity Strategy commits the administration "to engage with countries working in opposition to our larger agenda on common problems" even while building a "broad coalition of nations working to maintain an open, free, global, interoperable, reliable, and secure Internet."[37] As noted in recommendation 2.1, the Bureau of Cyberspace and Digital Policy will improve interagency coordination to build consensus with allies and partners on cyber norms.[38]

2.1.2 – Engage Actively and Effectively in Forums Setting International ICT Standards: *Nearing implementation/partial implementation via legislative action; further appropriations required.* The passage of the CHIPS and Science Act last summer triggered a cascade of efforts to create technical standards education and training resources and to partner with the private sector on emerging technologies.[39] A critical factor in the long-term success of this recommendation is the National Institute of Standards and Technology's (NIST's) capacity to promote the development of and coordination around international standards.

> ***"To increase the efficacy of cyber capacity building efforts and ensure resources are prioritized based on cyber-specific geopolitical considerations, funding for these efforts should be consolidated from regional programs to the State Department's Bureau of Cyberspace and Digital Policy (with some limited exceptions for law enforcement-related capacity building)."***

2.1.3 – Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance: *Nearing implementation/partial implementation via proposed legislation; further appropriations required.* The co-chairs continue to support increased and sustained appropriations to support cyber capacity building funds at the Department of State. Established in April 2022, the CDP is responsible for leading and coordinating the department's digital diplomacy efforts. To increase the efficacy of cyber capacity building efforts and ensure resources are prioritized based on cyber-specific geopolitical considerations, funding for these efforts should be consolidated from regional programs to CDP (with some limited exceptions for law enforcement-related capacity building).[40]

2.1.4 – Improve International Tools for Law Enforcement Activities in Cyberspace: *Implemented via executive action; funding appropriated*. While it was not explicitly earmarked for the FBI's Cyber Assistant Legal Attachés (ALATs) program, the president's FY24 budget includes an additional $63 million to "build cyber investigative capabilities at FBI field divisions nationwide."[41] While the recommendation is considered fully implemented, appropriators will need to continue to provide sustainment funding for the FBI's cyber mission.

2.1.5 – Leverage Sanctions and Trade Enforcement Actions: *Nearing implementation/partial implementation; further legislative action required.* The commission recommended Congress codify Executive Order 13848 on responding to foreign interference in the United States. While he has not taken this up, President Joseph Biden extended the authorities under the executive order by a year, delaying its expiration to September 2023.[42] Elsewhere, the executive branch continues to issue financial sanctions and enforcement actions to punish malicious cyber actors.

2.1.6 – Improve Attribution Analysis and the Attribution-Decision Rubric: *Nearing implementation/partial implementation; further executive action required.* One pillar of the National Cybersecurity Strategy is the disruption of threat actors. To this end, the strategy notes that the federal government has "established new diplomatic initiatives … to hold actors accountable" for malicious activity.[43] The strategy and its implementation plan do not identify additional initiatives to improve attribution analysis and speed, but there has been an observed improvement in U.S. and partner country attribution.

2.1.7 – Reinvigorate Efforts to Develop Cyber Confidence-Building Measures: *On track; further executive action required.* Establishing CDP and articulating the new National Cybersecurity Strategy advance this recommendation, but executive action requires a more focused effort. This may happen in the forthcoming International Cybersecurity Strategy.

Pillar 3: Promote National Resilience

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

3.1 – Codify Sector-Specific Agencies Into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk: *Fully implemented via legislative action; funds appropriated.* Congress codified sector risk management agencies (SRMAs) into law through the FY21 NDAA.[44] While some SRMAs still lack the resources, authorities, and leadership necessary to carry out their duties, there has been an uptick in SRMA-specific funding and programs in the past few years.[45] Following a congressionally mandated review of SRMA performance,[46] the Biden administration also announced it is reviewing and updating Presidential Policy Directive 21 (PPD-21) to improve critical infrastructure security.[47]

3.1.1 – Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy: *On track; awaiting legislative action.* This year, Senators Maggie Hassan (D-NH) and Mitt Romney (R-UT) re-introduced the National Risk Management Act of 2021[48] after the bill was omitted from the CHIPS and Science Act.[49] On March 29, 2023, the Senate Homeland Security and Governmental Affairs Committee voted to advance the bill to the Senate floor.[50] If passed, the bill would establish a process for CISA to study "cyber and physical threats to critical infrastructure" and require a report to Congress with recommendations to mitigate cyber risks.[51] The Department of Homeland Security would also lead risk identification and assessment in coordination with SRMAs, critical infrastructure owners and operators, the Office of the National Cyber Director, and other relevant parties to support the President's National Critical Infrastructure Resilience Strategy.

3.1.2 – Establish a National Cybersecurity Assistance Fund: *On track; awaiting legislative action.* In the Infrastructure Investment and Jobs Act, Congress created a $1 billion State and Local Cybersecurity grant program. In September 2022, DHS announced the first funding opportunity through this "first-of-its-kind" program.[52] While this grant program aligns with the intent of this recommendation, a National Cybersecurity Assistance Fund would address systemic cyber risks over a longer period of time.

3.2 – Develop and Maintain Continuity of the Economy (COTE) Planning: *Nearing/partial implementation via legislation; executive action necessary*. Congress implemented this recommendation in the FY21 NDAA, which required the president to report back to Congress within two years on the development of continuity of the economy plans. The White House belatedly delegated responsibility for this effort to CISA. The report transmitted to Congress concluded that the executive branch has many of the preparedness and response authorities and structures necessary for COTE. These plans, however, do not focus on economic recovery and do not involve the private sector in decision-making and implementation in the way that economic recovery planning necessitates. The report also fails to offer a process to ensure that planning documents and exercises are brought up to date with COTE requirements.

3.3 – Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund": *Fully implemented via legislative action and appropriated funds.* The Infrastructure Investment and Jobs Act of 2021 included the bipartisan Cyber Response and Recovery Act, implementing this recommendation.[53]

3.3.1 – Designate Responsibilities for Cybersecurity Services Under the Defense Production Act: *Nearing/partial implementation via executive action.* The Biden administration has continued using the Defense Production Act to protect supply chains for defense-critical goods.[54] Further executive action is required to include cybersecurity services as part of the bigger strategy to secure critical infrastructure supply chains.

3.3.2 – Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts: *Progress limited.* Commission staff had drafted legislation in support of this recommendation, but Congress for the third consecutive year has not introduced it.

3.3.3 – Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts: *Nearing implementation/partial implementation pending legislative action.* In January, CISA's Joint Cyber Defense Collaborative (JCDC) released its 2023 Planning Agenda, which notes that JCDC will lead the drafting of the National Cyber Incident Response Plan (NCIRP).[55] This announcement shows progress toward implementing the commission's original recommendation. The NCIRP must incorporate two elements: 1) outlining how federal, state, local, tribal, and territorial governments and private entities respond to significant cyber incidents affecting critical infrastructure, and 2) identifying options and resources to supplement the government's response. Integrating the two into existing emergency response and disaster recovery mechanisms is crucial.

3.3.4 – Expand Coordinated Cyber Exercises, Gaming, and Simulation: *Fully implemented via legislative action and appropriated funds.* The FY22 NDAA implemented this recommendation.[56] The FY23 omnibus spending bill appropriated $36.3 million for the National Infrastructure Simulation Analysis Center, a nearly $13.5 million increase from the previous year.[57] The funding remains available until September 30, 2024. In addition, the FY22 NDAA provides CISA with $6.5 million above the president's request to administer the National Cyber Exercise Program.[58]

3.3.5 – Establish a Biennial National Cyber Tabletop Exercise: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation.[59] CISA's Cyber Storm VIII exercise took place in March 2022, and its successor, Cyber Storm IX: National Cyber Exercise, is scheduled to take place in spring 2024.[60]

3.3.6 – Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard: *On track; pending report to Congress.* Section 1729 of the FY21 NDAA addressed this recommendation,[61] but the National Guard report evaluating rules and standards pertaining to the guard's use in response to a cyber incident was incomplete. Despite this, there has been meaningful improvement in the guard's capabilities to protect critical infrastructure. In 2022, 5,000 guard personnel provided cybersecurity support ahead of the midterm elections.[62] Clear guidance on the utilization of National Guard capabilities will be needed to fully address this recommendation.

> ***"The FY23 omnibus spending bill provided $28 million to the Election Assistance Commission (EAC). The EAC should update the Voluntary Voting System Guidelines before the 2024 election, and Congress should amend the Help America Vote Act to add a fifth nonpartisan commissioner with a cybersecurity background."***

3.4 – Improve the Structure and Enhance Funding of the Election Assistance Commission (EAC): *Nearing/partial implementation; legislative actions required.* The FY23 omnibus spending bill provided $28 million to the EAC, an $8 million increase from $20 million in FY22 funding. The FY23 bill also includes $75 million in funding for the Election Security Grants.[63] In addition, the president's FY24 budget request includes $5 billion to support state and local government election infrastructure.[64] Two items remain for full implementation of this recommendation, and they should remain a high priority. The EAC should update the Voluntary Voting System Guidelines before the 2024 election, and Congress should amend the Help America Vote Act to add a fifth nonpartisan commissioner with a cybersecurity background.

3.4.1 – Modernize Campaign Regulations to Promote Cybersecurity: *Progress limited; further legislative action required.* There has been limited progress in amending the Federal Election Campaign Law to allow corporations to provide free or reduced-cost cybersecurity assistance to political campaigns on a nonpartisan basis. CISA and nonprofit organizations, however, provide election security resources. While this differs from the commission's recommendations, the effort broadly aligns with the intent of this recommendation.[65]

3.5 – Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations: *On track via executive action; further executive action and appropriations required.* The Biden administration released the National Cybersecurity Workforce and Education Strategy outlining a comprehensive strategy for improving cyber education and workforce needs in the United States.[66] The first pillar of the strategy is "equip[ping] every American with foundational cyber skills" with three core components: digital literacy, computational literacy, and digital resilience.[67] Last year, the Department of Defense also requested $132 million for the National Defense Education Program, which includes a pilot program for civics education. The commission had recommended increased funding for this program. The FY22 spending bill did not provide funds for this program, but the FY23 NDAA authorized $140 million.[68]

3.5.1 – Reform Online Political Advertising to Defend Against Foreign Influence in Elections: *On track; legislation introduced.* Senators Amy Klobuchar (D-MN) and Lindsey Graham (R-SC) reintroduced the Honest Ads Act, a bill that would combat foreign interference in American elections and improve transparency of online political advertisements through Federal Election Commission oversight.[69] CSC co-chair, Representative Mike Gallagher (R-WI), and Representative Derek Kilmer (D-WA) introduced a companion bill in the House.[70]

Pillar 4: Reshape the Cyber Ecosystem Toward Greater Security

Reshape the Cyber Ecosystem toward Greater Security				
Rec. Number	**Recommendation Title**	**2021**	**2022**	**2023**
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: *Nearing implementation via executive action.* In July, the White House announced a new initiative, dubbed the U.S. Cyber Trust Mark, led by the Federal Communications Commission, to create a voluntary cybersecurity labeling program for Internet of Things consumer devices.[71] Once implemented, this labeling effort would inform consumers about the cybersecurity risks of IoT products, identifying products that voluntarily employ better cybersecurity practices.

4.1.1 – Create or Designate Critical Technology Security Centers: *Nearing/partial implementation via legislative action; further legislative action required.* This recommendation was partially implemented through appropriations from the Infrastructure Investment and Jobs Act to the Department of Homeland Security's Science and Technology Directorate.[72] In April, based on this recommendation, Representative Ritchie Torres (D-NY) also introduced the Critical Technology Security Centers Act of 2023,[73] which would establish and fund two centers to test the security of devices, identify vulnerabilities, and develop mitigation measures to certify secure technologies.[74]

4.1.2 – Expand and Support the National Institute of Standards and Technology Security Work: *Fully implemented via appropriations.* As noted earlier in Recommendation 2.1.2, the FY23 omnibus spending bill appropriated $1.65 billion to the National Institute on Standards and Technology.[75] This includes a $2 million increase above the FY22 enacted level for addressing cybersecurity issues of "industrial control systems devices procured by the Federal government."[76] In total, NIST's cybersecurity and privacy mission saw an increase of $20 million after years of underfunding.[77]

4.2 – Establish Liability for Final Goods Assemblers: *Progress limited/delayed.* Previously, this recommendation appeared to face significant hurdles. Strategic objective 3.3 of the National Cybersecurity Strategy, however, states that the administration will work with Congress and the private sector to develop legislation that would establish liability for software products and services.[78] The National Cybersecurity Strategy Implementation Plan notes that the ONCD will host a legal symposium to explore different approaches to implementing a software liability framework by the second quarter of FY24.[79]

4.2.1 – Incentivize Timely Patch Implementation: *Nearing/partial implementation via executive action.* As part of a series of steps to incentivize private companies to implement software patches in a timely manner, the commission recommended that the National Institute on Standards and Technology (NIST) update SP 800-40, the Guide to Enterprise Patch Management Technologies. NIST released the updated revision of the document in April 2022.[80]

4.3 – Establish a Bureau of Cyber Statistics: *On track; additional legislative action required.* Last year, then Representative Jim Langevin (D-RI) introduced the recommendation as an amendment to the FY23 NDAA, but it was not included in the final bill.[81] This year's NDAA could prompt renewed movement. Section 1715 of the Senate version of the bill requires the Department of Defense to conduct an assessment on establishing and resourcing the Office of Cyber Statistics as part of the cyber incident reporting requirement.[82] If the provision remains in the final bill, the resulting report could provide crucial information for fulfilling this recommendation.

4.4 – Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications: *Progress limited/delayed.* At this time, there remains limited executive action toward directing a federally funded research and development center to develop a training and certification program for insurance professionals.

4.4.1 – Establish a Public-Private Partnership on Modeling Cyber Risk: *On track via executive action and appropriations.* This recommendation will require executive action for full implementation, but progress is being made with various public-private partnerships. The newest efforts within CISA's Joint Cyber Defense Collaborative include exploring the potential for developing a new public-private "operational collaboration" in modeling cyber risk.[83]

4.4.2 – Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events: *Nearing/partial implementation via executive action.* In June 2023, the Department of the Treasury released an assessment of the competitiveness of small insurers in the terrorism risk insurance market.[84] As part of the implementation of the National Cybersecurity Strategy, Treasury's Federal Insurance Office will lead an effort to assess the need for "a federal insurance response to catastrophic cyber events."[85]

4.4.3 – Incentivize Information Technology Security Through Federal Acquisition Regulations and Federal Information Security Management Act Authorities: *Fully implemented via executive action.* The Biden administration implemented this recommendation in 2021 through Executive Order 14028, "Improving the Nation's Cybersecurity." In addition, the Senate Homeland Security and Government Affairs Committee advanced the Federal Information Security Modernization Act of 2023 in July.[86] This legislation would also achieve the intent of this recommendation.

4.4.4 – Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements: *Fully implemented via legislative action.* In July, the U.S. Securities and Exchange Commission adopted new rules requiring publicly traded U.S. companies and foreign private issuers to disclose material cybersecurity incidents and update their cybersecurity risk management policies and procedures, strategy, and governance annually.[87]

4.5 – Develop a Cloud Security Certification: *Nearing/partial implementation via legislative action; additional executive action necessary.* In the FY23 NDAA, Congress authorized the Federal Risk and Authorization Management Program (FedRAMP) to standardize security assessment of cloud computing products and services used for unclassified federal information.[88]

4.5.1 – Incentivize the Uptake of Secure Cloud Services for Small- and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments: *Nearing/partial implementation via legislative action.* The State and Local Cybersecurity Improvement Act, passed into law in the Infrastructure Investment and Jobs Act, partially implemented this recommendation.[89] In August 2023, the nonprofit Center for Internet Security launched a multi-cloud security compliance program with Microsoft to strengthen state, local, tribal, and territorial governments' cybersecurity infrastructure. The Center for Internet Security has collaborated with the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers since 2010.[90] While both of these programs align with the intent of this recommendation, they do not include small- and medium-sized businesses.

4.5.2 – Develop a Strategy to Secure Foundational Internet Protocols and Email: *Nearing/partial implementation via legislative action.* 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. The FY21 and FY22 NDAAs addressed some components of these elements.[91] In September 2022, CISA announced a new program for federal civilian agencies to protect against cyberattacks compromising DNS infrastructure.[92] Additional action is necessary to address the security of the Border Gateway Protocol.

4.5.3 – Strengthen the U.S. Government's Ability to Take Down Botnets: *On track via executive action.* The National Cybersecurity Strategy highlights law enforcement's collaboration with private industry and allies and partners to disable botnets and commits to continuing and expanding on this approach.[93] Additional legislation, as recommended by the commission, may be necessary to provide law enforcement with the authority to disrupt botnets engaged in a range of abusive behaviors.

In July, the U.S. Securities and Exchange Commission adopted new rules requiring publicly traded U.S. companies and foreign private issuers to disclose material cybersecurity incidents and update their cybersecurity risk management policies. SEC Chairman Gary Gensler (pictured above) said the rules will enhance and standardize disclosures to investors. (Photo by Alex Wong via Getty Images)

4.6 – Develop and Implement an Information and Communications Technology Industrial Base Strategy: *Nearing/partial implementation via executive action.* In July, the Commerce and Defense departments signed a memorandum of agreement to expand information sharing to "strengthen the semiconductor defense industrial base" related to provisions of the CHIPS and Science Act.[94] This statute and other executive action[95] had partially implemented this recommendation.[96] In March, the Pentagon submitted a report to Congress examining domestic industrial capabilities as required by a 2021 executive order on supply chains. The report's section on microelectronics includes recommendations to bolster domestic and allied production.[97] Further executive action is required to implement these recommendations.

4.6.1 – Increase Support to Supply Chain Risk Management Efforts: *Fully implemented via executive and legislative actions.* The February 2021 executive order and the passage of the CHIPS and Science Act fully implemented this recommendation.[98] In April 2023, CISA also announced a new national supply chain partnership with other federal and industry partners "to raise awareness on the importance of supply chain resilience."[99]

4.6.2 – Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies: *Fully implemented via legislative actions.* The passage of the CHIPS and Science Act fully implemented this recommendation.[100] Congressional appropriators have also provided consistent funding for this purpose. The FY23 omnibus spending bill, for example, appropriated funds for the Defense Department to test and evaluate emerging technologies and for the Commerce Department to create new jobs and apprenticeships in science, technology, engineering, and mathematics fields.[101]

4.6.3 – Strengthen the Capacity of the Committee on Foreign Investment in the United States: *Nearing/partial implementation via appropriations.* The FY23 omnibus spending bill provided the Committee on Foreign Investment in the United States (CFIUS) with $21 million,[102] a modest one million dollar increase from the FY22 enacted level.[103] Last September, the president issued a new executive order expanding the factors CFIUS uses during its review process to include cybersecurity, personal sensitive data, and other national security factors.[104] While the executive order does not grant CFIUS additional legal jurisdiction, it improves the foreign investment review process in terms of protecting U.S. competitiveness.

4.6.4 – Invest in the National Cyber Moonshot Initiative: *Partial implementation via legislative action.* The FY21 NDAA and the CHIPS and Science Act partially implemented this recommendation.[105] These statutes established new offices and guidelines for cyber threat assessment in the defense industrial base and included cyber education initiatives, meeting some of the goals of the Cyber Moonshot.

4.7 – Pass a National Data Security and Privacy Protection Law: *On track via executive and legislative action.* Various strategic objectives in the National Cybersecurity Strategy work to protect consumer privacy and sensitive information.[106] Meanwhile, on Capitol Hill, after Congress failed to pass data privacy legislation last year, the House Energy and Commerce Committee resumed discussions in March on the need for a federal data privacy bill.[107]

"Various strategic objectives in the National Cybersecurity Strategy work to protect consumer privacy and sensitive information. Meanwhile, on Capitol Hill, after Congress failed to pass data privacy legislation last year, the House Energy and Commerce Committee resumed discussions in March on the need for a federal data privacy bill."

4.7.1 – Pass a National Breach Notification Law: *Limited legislative and executive progress.* Legislative and executive actions in recent years reveal shifting attitudes toward national breach notification.[108] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), for example, is not a national breach notification law but does implement a separate commission recommendation.[109]

Pillar 5: Operationalize Cybersecurity Collaboration With the Private Sector

Operationalize Cybersecurity Collaboration With the Private Sector				
Rec. Number	**Recommendations Title**	**2021**	**2022**	**2023**
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": *On track via executive action and appropriations; further action required.* This has been a priority for the congressional members of the commission in recent years. Despite the inclusion of systemically important entities (SIEs) provision in the House version of the FY23 NDAA,[110] it was ultimately dropped from the final. Last September, CISA's Cybersecurity Advisory Committee recommended that the agency begin identifying SIEs.[111] CISA Director Jen Easterly partially accepted this suggestion, noting that "identifying SIEs is important to prioritize government resources and assets to prevent, mitigate and respond to risks to the most critical entities" and that CISA will coordinate with sector risk management agencies to develop an initial list of SIEs and create a program to engage these entities.[112] The FY23 omnibus spending bill allocated $1.8 million above the request to support CISA's work with SIEs.[113] Members of Congress have shown great interest in CISA's work on SIEs,[114] requesting updates on establishing a new program office dedicated to this work.

5.1.1 – Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector: *On track via executive action.* The National Security Agency is projecting that it will nearly triple its partnerships with the private sector, growing from 110 to more than 300 relationships by the year's end.[115] The agency has also doubled its analytical exchanges with private sector partners, including "10,000 bidirectional collaborations" and the sharing of dozens of zero-day vulnerabilities with companies.[116] Through these collaborations, the National Security Agency provides the private sector partners details of nation-state adversaries' activities, thereby better equipping them to protect against potentially catastrophic cybersecurity incidents.

5.1.2 – Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities: *On track; legislative action required.* In August, the Office of the Director of National Intelligence published its 2023 National Intelligence Strategy,[117] which notes that the intelligence community must "adopt new approaches" and "build new and restructure existing collaborative mechanisms with non-state actors" to protect U.S. critical infrastructure.[118]

5.1.3 – Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by providing CISA with administrative subpoena authority.[119]

5.2 – Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information: *On track; further legislative action required.* Despite inclusion of a provision to establish a joint collaborative environment in the House version of the FY23 NDAA, the provision again did not make it into the final version of the legislation.[120] Earlier this year, however, Aastha Verma, the chief of the Cybersecurity Division at CISA, noted that CISA is rolling out the Joint Collaborative Environment project to improve information exchange with the private sector.[121] While Congress ultimately removed the Joint Collaborative Environment provision from the final FY23 NDAA, the law does require the National Security Agency to conduct a study on the issue.[122] More significantly, the omnibus appropriations bill included funding to set up a collaborative environment at CISA.[123] The president's FY24 budget request includes $3 million for this effort.[124]

5.2.1 – Expand and Standardize Voluntary Threat Detection Programs: *Fully implemented via legislative action and appropriations.* The FY22 NDAA codified CyberSentry, a voluntary program administered by CISA that provides continuous monitoring and detection of cybersecurity threats on critical infrastructure networks.[125] The FY23 omnibus spending bill provided $31 million for threat hunting, of which $28 million was allocated to support CyberSentry, $3 million above the president's request.[126]

5.2.2 – Pass a National Cyber Incident Reporting Law: *Fully implemented via legislative action and appropriations.* The passage of CIRCIA as part of the FY22 consolidated appropriations bill fully implemented this recommendation.[127] The FY23 omnibus spending bill provided CISA with $23.4 million to carry out its duties as mandated by CIRCIA.[128] CISA is developing incident reporting rules for covered entities, and the National Cybersecurity Strategy Implementation Plan says that CISA will issue the final rule by the end of FY25.[129]

5.2.3 – Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors: *Progress limited.* The commission proposed an amendment to the Pen Register Trap and Trace Device Statute. While the commission shared with members of Congress draft legislative text supporting this recommendation in 2021, progress has been limited.

5.3 – Strengthen an Integrated Cyber Center Within CISA and Promote the Integration of Federal Cyber Centers: *Nearing/partial implementation via executive and legislative action.* Strategic objective 1.3 of the National Cybersecurity Strategy states that the federal government should integrate cybersecurity centers that "fuse together … homeland defense, law enforcement, intelligence, diplomatic, economic, and military" capabilities.[130] The Office of the National Cyber Director will lead the efforts to assess and improve federal cybersecurity centers by identifying gaps in capabilities by the end of FY23.[131] Previously, the FY21 NDAA requested a report on federal cybersecurity coordination,[132] but an update is pending.

5.4 – Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency: *Fully implemented via legislative action; funds appropriated.* The FY21 NDAA fully implemented this recommendation.[133] Now known as CISA's Joint Cyber Defense Collaborative, Congress continues to provide appropriations support for this effort.[134]

5.4.1 – Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives: *Fully implemented via legislative action; funds appropriated.* The FY22 NDAA implemented this recommendation,[135] and the Defense Department has taken an active role in fostering public-private partnerships over the past year. Some of the progress includes creating information exchange programs at the U.S. Cyber Command[136] and developing a pilot apprenticeship exchange program with the private sector.[137] There has been a high-level cultural shift within the department towards working with the private sector.[138]

5.4.2 – Expand Cyber Defense Collaboration With ICT Enablers: *Fully implemented via legislative action.* The FY22 NDAA created voluntary and pilot programs that implemented this recommendation.[139] Over the long term, more action might be necessary to ensure collaboration solidifies.

Pillar 6: Preserve and Employ the Military Instrument of Power

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

6.1 – Direct DoD to Conduct a Force Structure Assessment of the Cyber Mission Force: *Fully implemented via legislative action.* The FY21 NDAA mandated a force structure assessment that meets the intent of this recommendation.[140] In December, the Cyber National Mission Force became a subordinate unified command, reflecting its operational success.[141] The president's FY24 budget requests $13.5 billion for U.S. Cyber Command, expanding the number of Cyber Mission Force teams from 142 to 147, indicating some force structure assessment has occurred and shortfalls were being addressed.[142] A formal force structure assessment submitted to Congress (as previously requested) would be helpful in determining proper force generation requirements for the military services.

6.1.1 – Direct DoD to Create a Major Force Program Funding Category for U.S. Cyber Command: *Fully implemented via legislative actions.* The FY21 and FY22 NDAAs implemented this recommendation by eliminating the spending cap on programs and personnel and providing the Commander of U.S. Cyber Command with full budget authority.[143]

6.1.2 – Expand Current Malware Inoculation Initiatives: *On track; executive or legislative action required.* Various interagency efforts have disclosed information about malware[144] and indicators of compromise[145] to the public as these agencies encounter them through threat hunting or other similar activities. This has become a regular part of Cyber Command, law enforcement, and intelligence community activities. As the commission noted in its March 2020 report, the establishment of a Joint Collaboration Environment would accelerate such efforts.

6.1.3 – Review the Delegation of Authorities for Cyber Operations: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by delegating cyber-related authorities to the commander of U.S. Cyber Command.[146]

6.1.4 – Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces: *Progress limited.* There has been limited progress on this recommendation despite U.S. Cyber Command's active role in assisting international allies and partners, like Ukraine, to defend their networks following the February 2022 invasion of Ukraine. Executive action is required to update the Standing Rules of Engagement and Standing Rules for the Use of Force for U.S. forces.

6.1.5 – Cooperate With Allies and Partners to Defend Forward: *Fully implemented via executive action.* Since 2018, U.S. Cyber Command has conducted more than 40 missions in 21 countries.[147] In May 2023, the Defense Department released an unclassified summary of its cyber strategy, which states that the U.S. Cyber Command will continue to assist allies and partners in defending their networks through hunt forward missions.[148]

6.1.6 – Require DoD to Define Reporting Metrics: *On track via legislative action.* The FY20 NDAA required the Department of Defense to establish metrics to inform quarterly readiness assessments of the Cyber Mission Force.[149] The commission recommended additional steps to measure outcomes, a step that could be required by legislation or taken up through executive action. In the 2023 posture statement, General Paul Nakasone stated that U.S. Cyber Command's success is defined "by how effectively foreign adversarial actors are prevented from achieving their strategic objectives."[150] U.S. Cyber Command has grown in size and capabilities over the years, and further improvements to its force capabilities will require metrics to measure its effectiveness.

6.1.7 – Assess the Establishment of a Military Cyber Reserve: *Partially implemented via legislative action, additional executive action necessary.* The FY21 NDAA requires the Defense Department to evaluate "a reserve force dedicated to cyber issues."[151] It is unclear if the department has submitted its evaluation to Congress. In March 2023, Senators Marsha Blackburn (R-TN) and Jacky Rosen (D-NV) announced they would introduce legislation to create a pilot program for a civilian cybersecurity reserve force.[152] The bill is included in the Senate version of the FY24 NDAA.[153]

6.1.8 – Establish Title 10 Professors in Cyber Security and Information Operations: *On track via executive action.* The FY22 NDAA[154] partially implemented this recommendation. At the Armed Forces Communications and Electronics Association International's TechNet event, Lieutenant General Maria Barrett stated that U.S. forces must receive further education on cybersecurity.[155] This is a theme of the Pentagon's cyber workforce strategy.[156]

6.2 – Conduct a Cybersecurity Vulnerability Assessment Across the Nuclear Command, Control, and Communications and National Leadership Command Capability Systems and Continually Assess Weapon Systems' Cyber Vulnerabilities: *Fully implemented via executive and legislative action.* Multiple pieces of legislation[157] and executive action[158] mandate a wide array of actions to review, evaluate, and develop a secure nuclear command, control, and communications system.[159] This recommendation is considered fully implemented.

6.2.1 – Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program: *Nearing/partial implementation.* The FY21 NDAA[160] partially implemented this recommendation by requiring an assessment of the viability of a threat information sharing program for the defense industrial base (DIB). Two years later, the FY23 NDAA[161] limited the availability of certain funds until congressional committees receive the cybersecurity assessments of the DIB, as required by the FY21 NDAA. In May, the Defense Department issued a proposed rule that would revise the eligibility criteria for the voluntary DIB Cybersecurity Program requirements, thereby broadening the community for bilateral threat information sharing.[162]

6.2.2 – Require Threat Hunting on Defense Industrial Base Networks: *Nearing/partial implementation.* The FY21 NDAA[163] partially implemented this recommendation by requiring an assessment of the feasibility of implementing a cybersecurity threat hunting program for the defense industrial base.

6.2.3 – Designate a Threat-Hunting Capability Across the DoD Information Network: *Fully implemented via legislative action.* The FY22 NDAA implemented this recommendation by requiring threat hunting and discovery of malicious activity across the Defense Department's information network.[164]

6.2.4 – Assess and Address the Risk to National Security Systems Posed by Quantum Computing: *Fully implemented via legislative action.* The FY21 NDAA implemented this recommendation by requiring an assessment of the potential threats and risks posed by quantum computing.[165] Since then, there have been various other efforts to improve the understanding of quantum computing's possible threats to U.S. national security systems. For example, the Pentagon's 2022 annual report to Congress on security developments involving China assesses Beijing's quantum computing capabilities.

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**
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 Governments and Small- and Medium-Sized Businesses Information Technology Modernization Grants: *Fully implemented via legislative action.* The State and Local Cybersecurity Improvement Act, passed as part of the Infrastructure Investment and Jobs Act, implemented this recommendation.[166] For FY23, CISA and the Federal Emergency Management Agency made $374.9 million in grant funding available for this effort.[167] The Pentagon's Office of Strategic Capital and the Small Business Administration also announced a collaboration on the Small Business Investment Company Critical Technologies initiative.[168]

Pandemic 1.2 – Pass an Internet of Things Security Law: *Nearing/partial implementation via executive action.* In July 2023, the administration announced a cybersecurity certification and labeling program to help protect American consumers from potential cyber risks associated with IoT devices.[169] The details of this executive action are noted under Recommendation 4.1 in this report.

Pandemic 1.3 – Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts: *Progress limited; legislative action required.* A GAO report emphasized that federal agencies face challenges in standardizing metrics for reporting cybercrime. This may make it more difficult for nongovernmental organizations to aid in this effort, considering that it is still not mandatory for victims to self-report, and commitment to the use of the National Incident-Based Reporting System varies.[170] This GAO report comes a year after the introduction of the "Better Cybercrime Metrics Act."[171] The Cyber Peace Institute's Humanitarian Cybersecurity Center initiative[172] and Cybercrime Support Network are good examples of such efforts.

Pandemic 1.4 – Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns: *On track via various funding opportunities*. Earlier this year, the Department of State's Global Engagement Center released a $1 million notice of funding opportunity to research strategies to counter Russian disinformation and propaganda.[173] In June, the National Science Foundation requested proposals for a workshop to discuss research security threats, including disinformation and foreign influence.[174] For full implementation of the recommendation, Congress should authorize and appropriate funds for grant programs at the departments of Justice and Homeland Security and the National Science Foundation to support federal and international partners' research efforts.

Pandemic 1.4.1 – Establish the Social Media Data and Threat Analysis Center: *Nearing/partial implementation via legislative action.* The FY23 NDAA directed the director of national intelligence to submit "a plan to operationalize" the Social Media and Threat Analysis Center.[175] The requested plan has not yet been submitted to congressional committees.

White Paper #2: National Cyber Director

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

Establish a National Cyber Director: *Fully implemented via legislative and executive action; funding appropriated.* The FY21 NDAA created the Office of the National Cyber Director.[176] Since then, the office staff has grown, and the FY23 omnibus spending bill authorized $22 million for the expansion of the office.[177] The office led the drafting of the National Cybersecurity Strategy and the National Cybersecurity Workforce and Education Strategy, providing two strategy documents to coordinate cybersecurity efforts across the federal government. The administration belatedly named a successor to Director Chris Inglis following his departure in February. The new nominee, Harry Coker, Jr., is awaiting Senate confirmation.[178]

White Paper #3: Growing a Stronger Federal Cyber Workforce

Growing a Stronger Federal Cyber Workforce				
Rec. Number	**Recommendation Title**	**2021**	**2022**	**2023**
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: *Nearing implementation/partial implementation; further executive action required.* This recommendation calls for two bodies to lead and coordinate federal cybersecurity workforce development efforts — a Cyber Workforce Steering Committee and a Cyber Workforce Coordinating Working Group.[179] There have been various efforts that partially implement this recommendation. In December, the Office of the National Cyber Director established "the principal interagency forum" known as the National Cyber Workforce Coordination Group, comprising federal agencies and chaired by the ONCD, to address the federal workforce and education challenges.[180] In August, the ONCD published the National Cybersecurity Workforce and Education Strategy, which states that the office "will explore the establishment of a standing advisory committee."[181]

Workforce 2 – Properly Identify and Utilize Cyber-Specific Occupational Classifications: *On track with further executive actions required.* The FY22 NDAA calls on the Office of Personnel Management to update the occupational series system for technology-related positions. These updates are still pending.[182] In July, the office published a memo listing a set of general and technical competencies along with the definitions of competencies deemed necessary for artificial intelligence-related federal government positions.[183] According to the National Cybersecurity Workforce and Education Strategy, the Office of the National Cyber Director and National Cyber Workforce Coordination Group will continue to collect data and lead research efforts to update the occupational series to accurately reflect the skillsets needed within the federal government.

Workforce 3 – Develop Apprenticeships: *Nearing implementation/partial implementation via partial executive and legislative action.* According to the National Cybersecurity Workforce and Education Strategy, the Office of the National Cyber Director and its Federal Cyber Workforce Working Group will explore establishing a Federal Cyber Workforce Development Institute to provide pathways into federal cybersecurity positions and upskilling and reskilling for early-career talent development and mid to late-career talent.[184] The FY23 omnibus appropriations bill provided funds for various cybersecurity apprenticeship programs at CISA.[185] Successful implementation of the recommendation will require creating new programs and resourcing existing ones to build new pathways into the cyber workforce.

Workforce 4 – Improve Cybersecurity for K-12 Schools: *Nearing implementation/partial implementation; further executive and legislative action required.* In January, CISA published a report outlining cybersecurity risks facing educational institutions and providing guidelines, recommendations, and resources for schools. The K-12 Cybersecurity Act of 2021 required CISA to develop the report and host a series of roundtables that informed its contents.[186] In August, the White House also announced a series of actions to reinforce K-12 cybersecurity over the next three years.[187]

Workforce 5 – Provide Work-Based Learning via Volunteer Clinics: *Nearing implementation/partial implementation; further executive or legislative action required.* In June, Google announced a $20 million initiative to expand cybersecurity clinics in collaboration with the nonprofit Consortium of Cybersecurity Clinics.[188] Similar to the goal of this recommendation, the fund aims to expand the accessibility of educational opportunities and real-world experience for members of underserved communities. While the recent National Cybersecurity Workforce and Education Strategy supports cyber clinics' work directly within local communities,[189] long-term effectiveness may require congressional authorizations and further appropriations.

The Office of the National Cyber Director, led by Acting Director Kemba Walden (pictured above), released the National Cybersecurity Workforce and Education Strategy in July in line with many CSC recommendations. (Photo by Brittany Murray/MediaNews Group/ Long Beach Press-Telegram via Getty Images)

Workforce 6 – Improve Pay Flexibility and Hiring Authorities: *On track with some executive action taken; further executive and legislative actions required.* The Biden administration continued efforts to improve pay flexibility and hiring authorities for federal cyber employees this year. The National Cybersecurity Workforce and Education Strategy states that the White House will "work with Congress" to establish pay flexibility and hiring authorities across the federal government.[190] The Office of Personnel Management also approved a Special Salary Rate (SSR) for federal information technology and cybersecurity jobs in February.[191] The step, however, was met with pushback from some departments including Defense.[192] Coordination across the federal departments and agencies, along with legislative action, will be needed for this recommendation to be fully implemented.

Workforce 7 – Incentivize Cyber Workforce Research: *Implemented via legislative action and appropriations.* The passage of the CHIPS and Science Act fully implemented this recommendation last year. Additionally, the president's FY24 budget requests $11.35 million for the National Center for Science and Engineering Statistics to support activities to collect increased data on the cybersecurity workforce.[193]

Workforce 8 – Mitigate Retention Barriers and Invest in Diversity, Equity, and Inclusion in Recruiting: *Nearing implementation/partial implementation via executive order; further executive action and appropriations required.* Since the issuance of the June 2021 Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce, the Biden administration has prioritized issues around diversity in the federal workforce writ large. Specifically on the federal cyber workforce, the Office of Personnel Management released a Cyber Workforce Dashboard,[194] which makes demographic data for cybersecurity jobs across the federal government accessible. Provisions in the CHIPS and Science Act also support research into cyber workforce demographics and issues affecting employee recruitment and retention.[195] On retention issues, in the FY23 NDAA, Congress authorized $750,000 in appropriations over five years for the Office of Personnel Management's cybersecurity program to establish a Global Talent Management team dedicated to recruiting and retaining candidates with backgrounds in cybersecurity and various critical technologies.[196]

White Paper #4: Building a Trusted ICT Supply Chain

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

Supply Chain 1 – Develop and Implement an ICT Industrial Base Strategy: *Fully implemented via executive action.* Previously, this recommendation was considered fully implemented with the issuance of the February 2021 supply chain executive order. Over the past year, the Biden administration has continued to prioritize securing information and communications technology supply chains. For example, in February 2023, President Biden authorized the use of the Defense Production Act to support the production of microelectronics and integrated circuits.[197]

Supply Chain 2 – Identify Key Information and Communication Technologies and Materials: *Fully implemented via executive and legislative action; funding appropriated.* The February 2022 Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry fully implemented this recommendation.[198] Over the past year, Congress and the Biden administration have remained focused on this issue. The Department of State's budget requests $100 million for supply chain and information and communications technology security as appropriated through the CHIPS and Science Act.[199] Lawmakers, meanwhile, have requested security briefings on the threat posed by the Chinese Communist Party to these supply chains.[200]

Supply Chain 3 – Conduct a Study on the Viability of Critical Technology Clusters and Designate Them: *Fully implemented via legislative action and appropriations.* The passage of the CHIPS and Science Act established a regional technology and innovation hubs program at the Department of Commerce and authorized a similar program at the National Science Foundation.[201] This latter program provides awards to accredited U.S. higher education institutions, nonprofits, and for-profit organizations that partner with one or more minority-serving institutions.[202]

Supply Chain 3.1 – Provide Research and Development Funding for Critical Technologies: *Full implementation via legislative action and appropriations.* The CHIPS and Science Act implemented this recommendation and spurred additional investments in research and development for critical technologies. For example, in December, the National Telecommunications and Information Administration requested public comment on the implementation of a $1.5 billion grant program to invest in telecommunications infrastructure.[203]

Supply Chain 3.2 – Incentivize the Movement of Critical Chip and Technology Manufacturing Out of China: *Implemented via legislative action.* The CHIPS and Science Act provided more than $50 billion to incentivize U.S. domestic chip industry development.

Supply Chain 3.3 – Conduct a Study on a National Security Investment Corporation: *Progress limited; further executive and legislative action required.* The commission drafted legislation mandating a study assessing the possible impacts of establishing a National Security Investment Corporation. Congress has not yet taken up this legislation.

Supply Chain 4 – Designate a Lead Agency for ICT Supply Chain Risk Management: *Implemented via legislative action; further appropriations required.* The FY21 NDAA designated the Department of Homeland Security as the sector risk management agency for the information technology sector, fully implementing this recommendation.[204] The FY24 president's budget request, however, shows a reduction in CISA's funding request for sector risk management and sector stakeholder engagement.[205] While this recommendation is considered implemented, consistent funding for CISA to carry out its sector risk management agency duties is critical to protecting critical infrastructure.

Supply Chain 4.1 – Establish a National Supply Chain Intelligence Center: *On track; executive and legislative action required.* The CHIPS and Science Act authorizes a pilot program on domestic supply chain security, which the administration is using to create the national Supply Chain Optimization and Intelligence Network to map U.S. supplier capability and capacity, among other efforts.[206] This is aligned with the commission intent but does not itself implement this recommendation.

Supply Chain 4.2 – Fund Critical Technology Security Centers: *Partial implementation via legislation; further legislative action required.* The Infrastructure Investment and Jobs Act partially implements this recommendation by providing funds to the Department of Homeland Security's Science and Technology Directorate.[207] Full implementation will require passage of legislation creating critical technology security centers.

Supply Chain 5 – Incentivize Open and Interoperable Standards and Release More Mid-Band Spectrum: *Nearing implementation; further executive action required.* Full implementation of this recommendation is dependent upon the pending Defense Department study (as mandated in the Infrastructure Investment and Jobs Act) on repurposing the mid-band spectrum for commercial use and on actions to implement the findings of that study.[208] The Federal Communications Commission is also conducting a similar study.[209]

Supply Chain 5.1 – Develop a Digital Risk Impact Assessment for International Partners for Telecommunications Infrastructure Projects: *On track via executive action.* The Digital Connectivity and Cybersecurity Partnership initiative is an interagency effort that encourages international allies and partners to purchase secure information and communications technology products. While it does not provide a digital risk impact assessment, the program raises cybersecurity awareness among U.S. allies and partners.[210]

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: *Partially implemented via legislative action; further executive and legislative action required.* The CHIPS and Science Act partially implemented this recommendation.[211]

Supply Chain 5.3 – Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects: *On track; further executive and legislative action required.* Congress and the Biden administration remain focused on limiting the ability of certain Chinese state-controlled companies to do business in the United States and purchase national security-related U.S. goods and services. The administration has not developed a stand-alone list of entities barred from participating in U.S.-funded development projects, but the inclusion of a company on other U.S. entity lists restricts its ability to participate in these projects.

White Paper #6: Countering Disinformation in the United States

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

Countering Disinformation 1 – Establish a Civic Education Task Force, Enable Greater Access to Civic Education Resources, and Raise Public Awareness: *Nearing/partial implementation via legislative action; funding appropriated.* The FY23 omnibus spending bill boosted funding for civics education for K-12 schools, providing $23 million for this effort.[212] Among the topics, the bill mentions recognizing mis/disinformation.[213] The funded program activities meet the intent of this recommendation.[214] This year, the president's budget requests $73 million for American history and civics education programs, a $50 million increase from last year's enacted level.[215] Establishing a Civic Education Task Force and National Disinformation Awareness Outreach Program, however, will require new authorizing legislation.

Countering Disinformation 2 – Ensure Material Support for Nongovernmental Disinformation Researchers: *Nearing/partial implementation via appropriations.* As noted earlier in recommendation 1.4 of the pandemic white paper, there has been an increase in grant funding for disinformation research overall.[216] For instance, the National Science Foundation awarded a two-year, $5 million grant to create tools to help older adults recognize deceptive content and learn ways to protect themselves from online scams.[217]

Countering Disinformation 3 – Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public: *On track via various actions.* The Department of State and the National Science Foundation provided grant funding to research malign foreign influence campaigns. However, legislative action is required to authorize a new grant program administered by the Department of Justice to provide funding for nonprofit research on this topic.

Countering Disinformation 4 – Create a Capability Within DHS to Actively Monitor Foreign Disinformation: *Progress limited via legislative action.* The Department of Homeland Security created the Disinformation Governance Board in April 2022 but soon disbanded it in reaction to concerns of government censorship.[218]

Countering Disinformation 5 – Create a Grant Program to Equip State and Local Governments: *Nearing/partial implementation via appropriated funds.* The FY23 appropriations bill provides grants that align with this recommendation. However, a dedicated grant program with significantly more funding that provides state and local governments personnel and resources to identify foreign disinformation campaigns will require legislative action and appropriations.

Countering Disinformation 6 – Reform the Foreign Agents Registration Act (FARA) and Introduce New Federal Communications Commission Regulations: *On track via legislative action.* On February 15, Senator John Cornyn (R-TX) and a group of colleagues introduced the Preventing Adversary Influence, Disinformation and Obscured Foreign Financing Act, which would remove Foreign Agents Registration Act exemptions for foreign persons from China, Russia, Iran, North Korea, Cuba, or Syria.[219] If amended to further remove exemption for media entities, this legislation would implement the commission's original recommendation. Additionally, the U.S. Senate unanimously passed the Disclosing Foreign Influence Act co-sponsored by Senators Chuck Grassley (R-IA) and Maggie Hassan (D-NH).[220] If passed by the full Congress, the bill would require foreign governments and political parties that participate in lobbying efforts to disclose their activity.

Countering Disinformation 7 – Publish and Enforce Transparency Guidelines for Social Media Platforms: *Progress limited; further legislative action required.* Earlier this year, X, then known as Twitter, removed labels that inform social media users of accounts controlled or funded by governments, potentially increasing disinformation content.[221] While this recommendation does not require any content moderation, X's policy change exemplifies why lawmakers must keep social media companies accountable for policies on content removal, advertising, bot labeling, and other activities.

Conclusion

Since the publication of the commission's first annual assessment in August 2021, Congress and the Biden administration have undertaken a herculean effort to advance U.S. cybersecurity. With the release of the National Cybersecurity Strategy and its implementation plan, the path forward has become clearer, even if a long road ahead remains. For long-lasting success, cybersecurity initiatives require sustained funding, public-private partnerships, and international cooperation. The CSC's work as a government entity concluded with the white papers outlined above. However, the nonprofit CSC 2.0 project has conducted research extending from the commission's work, in addition to continuing research and analysis on existing recommendations. CSC 2.0 remains committed to providing an annual assessment of how the federal government is doing.

Endnotes

1. U.S. Senate Committee on Appropriations, "Summary of H.R. 1158 FY2020 Consolidated National Security Appropriations Package," December 2019, page 15. (https://www.appropriations.senate.gov/imo/media/doc/121619%20--%20HR1158%20Natl%20Security%20Package%20Summary.pdf)

2. U.S. House Committee on Appropriations, "Homeland Security," page 4. (https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/Homeland%20Security%20FY23%20Summary.pdf)

3. Mark Montgomery and Jiwon Ma, "President's cyber budget request is off to a good start; Congress should fill the gaps," *The Hill*, April 15, 2023. (https://thehill.com/opinion/cybersecurity/3952133-presidents-cyber-budget-request-is-off-to-a-good-start-congress-should-fill-the-gaps)

4. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4098. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

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

6. Ibid.

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

8. The White House, "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy Implementation Plan," July 13, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan)

9. Christian Vasquez, "White House releases National Cybersecurity Strategy implementation plan," *CyberScoop*, July 13, 2023. (https://cyberscoop.com/national-cybersecurity-strategy-implementation-plan-2)

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

11. Ibid., page 32.

12. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 2892. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf)

13. U.S. Congress, "Joint Explanatory Statement, Division I - Legislative Branch Appropriations Act 2021," 2020, page 2. (https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-I.pdf)

14. U.S. Government Accountability Office, "Fiscal Year 2024 Budget Request," March 15, 2023, pages 1-3. (https://www.gao.gov/assets/gao-23-900494.pdf)

15. Library of Congress, "Library of Congress Fiscal 2024 Budget Justification," page 127. (https://www.loc.gov/static/portals/about/reports-and-budgets/documents/budgets/fy2024.pdf)

16. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the President on NCD Nomination," May 11, 2023. (https://www.king.senate.gov/imo/media/doc/051123lettertopotusonncd.pdf)

17. The White House, "President Biden Announces Key Nominees," July 25, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/25/president-biden-announces-key-nominees-51)

18. U.S. Senate Committee on Appropriations, "FY23 Omnibus Appropriations Package Topline Summary," page 13. (https://www.appropriations.senate.gov/imo/media/doc/FY23%20Omnibus%20Full%20Summary.pdf)

19. @ericgeller, *X*, August 12, 2023. (https://twitter.com/ericgeller/status/1690512207497539584?s=46&t=tbm5OoJwp9K8b7-qrKN0AA)

20. National Defense Authorization Act for Fiscal Year 2023, H.R. 7900, 117th Congress (2022), §5214. (https://www.congress.gov/117/bills/hr7900/BILLS-117hr7900pcs.pdf)

21. The White House, "National Cybersecurity Strategy," March 1, 2023, page 16. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

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

23. The White House, "Budget of the U.S. Government Fiscal Year 2024," page 36. (https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf)

24. Federal Bureau of Investigation, "Federal Bureau of Investigation Budget Request for Fiscal Year 2024," April 27, 2023. (https://www.fbi.gov/news/testimony/federal-bureau-of-investigation-budget-request-for-fiscal-year-2024)

25. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1531. (https://www.congress.gov/bill/117th-congress/house-bill/4346)

26. U.S. Chief Human Capital Officers Council, "Guidance for Implementing Federal Rotational Cyber Workforce Program," March 17, 2023. (https://www.chcoc.gov/content/guidance-implementing-federal-rotational-cyber-workforce-program)

27. Office of Personnel Management. "Federal Rotational Cyber Workforce Program." (https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/federal-rotational-cyber-workforce-program)

28. Federal Cybersecurity Workforce Expansion Act, S. 2256, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/senate-bill/2256/actions)

29. Office of Senator Maggie Hassan, Press Release, "Senators Hassan, Cornyn Introduce Bipartisan Bill to Strengthen Federal Cyber Workforce," June 25, 2021. (https://www.hassan.senate.gov/news/press-releases/senators-hassan-cornyn-introduce-bipartisan-bill-to-strengthen-federal-cyber-workforce)

30. The White House, Press Release, "FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America's Cyber Talent," July 31, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent)

31. U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview: Fiscal Year 2023 Congressional Justification," March 2022, pages 174 and 176. (https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf)

32. U.S. Senate Committee on Appropriations. "Division F – Department of Homeland Security Appropriations Act, 2023," accessed September 8, 2023, page 56. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf)

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

34. 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)

35. Cate Burgan, "State Dept. to Deploy Global Cyber Officers by end of 2024," *MeriTalk*, April 12, 2023. (https://www.meritalk.com/articles/state-dept-to-deploy-global-cyber-officers-by-end-of-2024)

36. U.S. Department of State, "Congressional Budget Justification Appendix 1: Department of State Diplomatic Engagement Fiscal Year 2024," April 2023, page 280. (https://www.state.gov/wp-content/uploads/2023/04/FY-2024-CBJ-Appendix-1-Final_14-April-2023_-_.pdf)

37. The White House, "National Cybersecurity Strategy," March 1, 2023, page 29. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

38. Ibi

39. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1366. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

40. Mark Montgomery and Annie Fixler, "Building Partner Capabilities for Cyber Operations," *Foundation for Defense of Democracies*, July 27, 2023. (https://www.fdd.org/analysis/2023/07/27/building-partner-capabilities-for-cyber-operations)

41. The White House, "Budget of the U.S. Government Fiscal year 2024," page 36. (https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf)

42. Executive Order 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," September 12, 2018. (https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election); The White House, "Notice on the Continuation of the National Emergency With Respect to Foreign Interference In or Undermining Public Confidence in United States Elections," September 7, 2022. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/07/notice-on-the-continuation-of-the-national-emergency-with-respect-to-foreign-interference-in-or-undermining-public-confidence-in-united-states-elections-2)

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

44. 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)

45. Mary Brooks, Annie Fixler, and Mark Montgomery, "Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure," *CSC 2.0*, June 2023. (https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure)

46. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Section 9002(b) Report," November 12, 2021. (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf)

47. The White House, Press Release, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure," November 7, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure)

48. United States Innovation and Competition Act of 2021, S. 1260, 117th Congress (2021), §4461. (https://www.congress.gov/bill/117th-congress/senate-bill/1260)

49. National Risk Management Act of 2023, S. 824, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/senate-bill/824)

50. Office of Senator Maggie Hassan, Press Release, "Senate Committee Passes Hassan-Backed Bipartisan Bills to Strengthen Defenses Against Cyber and Potential Terrorist Attacks," March 29, 2023. (https://www.hassan.senate.gov/news/press-releases/senate-committee-passes-hassan-backed-bipartisan-bills-to-strengthen-defenses-against-cyber-and-potential-terrorist-attacks)

51. Congressional Budget Office, "S. 824, National Risk Management Act of 2023," April 17, 2023. (https://www.cbo.gov/system/files/2023-04/s0824.pdf)

52. U.S. Department of Homeland Security, Press Release, "Biden-Harris Administration Announces $1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program," September 16, 2022. (https://www.dhs.gov/news/2022/09/16/biden-harris-administration-announces-1-billion-funding-first-ever-state-and-local)

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

54. The White House, "Memorandum on Presidential Waiver of Statutory Requirements Pursuant to Section 303 of the Defense Production Act of 1950, as amended, on Department of Defense Supply Chains Resilience," February 27, 2023. (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/27/memorandum-on-presidential-waiver-of-statutory-requirements-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-department-of-defense-supply-chains-resilience)

55. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "JCDC Focused on Persistent Collaboration and Staying Ahead of Cyber Risk in 2023," January 26, 2023. (https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023); "2023 JCDC Planning Agenda," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed September 8, 2023. (https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2023-jcdc-planning-agenda)

56. 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)

57. U.S. Senate Committee on Appropriations, "Division F - Department of Homeland Security Appropriations Act, 2023," March 2023, page 54. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf); U.S. House Committee on Appropriations, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," March 2022, page 48. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

58. 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)

59. 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)

60. "Cyber Storm VIII: National Cyber Exercise," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed September 8, 2023. (https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise); "Cyber Storm IX: National Cyber Exercise," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed September 8, 2023. (https://www.cisa.gov/cyber-storm-ix-national-cyber-exercise)

61. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4118. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

62. Lauren C. Williams, "More Than a Dozen States Have Activated the National Guard to Secure Midterm Elections," *Defense One*, November 7, 2022. (https://www.defenseone.com/defense-systems/2022/11/more-dozen-states-have-activated-national-guard-secure-midterm-elections/379412)

63. U.S. Senate Committee on Appropriations, "Summary Financial Services and General Government Fiscal Year 2023 Appropriations Bill," December 19, 2022, page 3. (https://www.appropriations.senate.gov/imo/media/doc/FSGG%20FY%2023.pdf)

64. U.S. Election Assistance Commission, "Fiscal Year 2024 Congressional Budget Justification," accessed September 8, 2023, page 22. (https://www.eac.gov/sites/default/files/cbj/US_EAC_FY_2024_Congressional_Budget_Justification_FINAL.pdf)

65. "Cybersecurity Toolkit and Resources to Protect Elections," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed September 8, 2023. (https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections)

66. The White House, "FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America's Cyber Talent," July 31, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent)

67. Executive Office of the President, Office of the National Cyber Director, "National Cyber Workforce and Education Strategy," July 31, 2023, pages 8-9. (https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf)

68. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3147. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf)

69. Office of Senator Amy Klobuchar, Press Release, "Klobuchar, Graham, Warner Introduce Bipartisan Legislation to Improve Transparency and Accountability of Online Political Advertising," February 27, 2023. (https://www.klobuchar.senate.gov/public/index.cfm/2023/2/klobuchar-graham-warner-introduce-bipartisan-legislation-to-improve-transparency-and-accountability-of-online-political-advertising)

70. Office of Representative Mike Gallagher, Press Release, "Gallagher, Kilmer Introduce Bipartisan, Bicameral Legislation to Bring Transparency and Accountability to Online Political Ads," April 17, 2023. (https://gallagher.house.gov/media/press-releases/gallagher-kilmer-introduce-bipartisan-bicameral-legislation-bring-transparency)

71. The White House, Press Release, "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers," July 18, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers); Federal Communications Commission, "Notice of Proposed Rulemaking," August 10, 2023. (https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf)

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

73. Critical Technology Security Centers Act of 2023, H.R. 2866, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/house-bill/2866/text)

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

75. U.S. Senate Committee on Appropriations, "Summary Commerce, Justice, Science, and Related Agencies Subcommittee Fiscal Year 2023 Appropriations Bill," December 19, 2022, page 5. (https://www.appropriations.senate.gov/imo/media/doc/CJS%20FY%2023.pdf)

76. U.S. Senate Committee on Appropriations, "Division B – Commerce, Justice, Science, and Related Agencies Appropriations Act, 2023," accessed September 8, 2023, page 14. (https://www.appropriations.senate.gov/imo/media/doc/Division%20B%20-%20CJS%20Statement%20FY23.pdf)

77. U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2024 Budget Submission to Congress," March 2023, pages 34-35. (https://www.commerce.gov/sites/default/files/2023-03/NIST-NTIS-FY2024-Congressional-Budget-Submission.pdf)

78. The White House, "National Cybersecurity Strategy," March 1, 2023, pages 20-21. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

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

80. U.S. Department of Commerce, National Institute for Standards and Technology, "Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology," April 2022. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf)

81. Amendment to Rules Comm. Print 117-54, Homeland Security Act of 2002, 117th Congress (2021). (https://amendments-rules.house.gov/amendments/LANGEV_080_xml220705161024895.pdf)

82. National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Congress (2023), page 1142. (https://www.congress.gov/bill/118th-congress/senate-bill/2226)

83. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Connecting the Dots to Drive Down Cyber Risk Together: The Superheroes Behind the Nation's JCDC," August 12, 2022. (https://www.cisa.gov/news-events/news/connecting-dots-drive-down-cyber-risk-together-superheroes-behind-nations-jcdc)

84. U.S. Department of the Treasury, Press Release, "Treasury Releases Assessment of Small Insurer Competitiveness in the Terrorism Risk Insurance Marketplace," June 30, 2023. (https://home.treasury.gov/news/press-releases/jy1586)

85. The White House, "National Cybersecurity Strategy Implementation Plan," July 2023, page 34. (https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf)

86. Justin Doubleday, "FISMA reform bill moves forward in Senate, while CMMC goes to White House review," *Federal News Network*, July 26, 2023. (https://federalnewsnetwork.com/cybersecurity/2023/07/fisma-reform-bill-moves-forward-in-senate-while-cmmc-goes-to-white-house-review)

87. U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022. (https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf); 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)

88. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3449. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf); The Federal Risk and Authorization Management Program, "FedRAMP Announces the Passing of the FedRAMP Authorization Act!" January 11, 2023. (https://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act)

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

90. Keely Quinlan, "Center for Internet Security announces Microsoft partnership," *StateScoop*, August 11, 2023. (https://statescoop.com/center-internet-security-microsoft-partnership)

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

92. U.S. Department of Homeland Security, Critical Infrastructure and Security Agency, Press Release, "CISA Launches its Protective DNS Resolver with General Availability for Federal Agencies," September 27, 2022. (https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies)

93. The White House, "National Cybersecurity Strategy," March 1, 2023, pages 14-15. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

94. 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)

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

96. Ibid.

97. U.S. Department of Defense, Office of the Assistant Secretary of Defense for Sustainment, "Industrial Capabilities Report to Congress," March 2023. (https://www.businessdefense.gov/docs/resources/FY2021-Industrial-Capabilities-Report-to-Congress.pdf)

98. Executive Order 14017, "America's Supply Chains," February 24, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains); CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1478. (https://www.congress.gov/bill/117th-congress/house-bill/4346)

99. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA and Partners Launch National Supply Chain Integrity Month," April 3, 2023. (https://www.cisa.gov/news-events/news/cisa-and-partners-launch-national-supply-chain-integrity-month)

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

101. U.S. House Committee on Appropriations, "Consolidated Appropriations Act, 2023, Summary of Appropriations Provisions by Subcommittee," accessed September 8, 2023, pages 4 and 9. (https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/FY23%20Summary%20of%20Appropriations%20Provisions.pdf)

102. U.S. Senate Committee on Appropriations, "Division E - Financial Services and General Government Appropriations Act, 2023," accessed September 8, 2023, page 4. (https://www.appropriations.senate.gov/imo/media/doc/Division%20E%20-%20FSGG%20Statement%20FY23.pdf)

103. U.S. Senate Committee on Appropriations, "Division E - Financial Services and General Government Appropriations Act, 2022," accessed September 8, 2023, page 3. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-E.pdf)

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

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

106. The White House, "National Cybersecurity Strategy," March 1, 2023. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

107. American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2021), (https://www.congress.gov/bill/117th-congress/house-bill/8152/text); Gregory T. Parks and Ronald W. Del Sesto, Jr., "US Data Privacy Legislation: Could a Federal Law be on the Horizon?" *Morgan Lewis*, July 31, 2023. (https://www.morganlewis.com/pubs/2023/07/us-data-privacy-legislation-could-a-federal-law-be-on-the-horizon)

108. Data Breach Reporting Requirements, 88 Federal Register 3953, January 23, 2023. (https://www.federalregister.gov/documents/2023/01/23/2023-00824/data-breach-reporting-requirements); U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022. (https://www.sec.gov/rules/proposed/2022/33-11038.pdf)

109. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed September 8, 2023. (https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia)

110. National Defense Authorization Act for Fiscal Year 2023, H.R. 7900, 117th Congress (2022), §5207. (https://www.congress.gov/117/bills/hr7900/BILLS-117hr7900pcs.pdf)

111. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA Cybersecurity Advisory Committee September 13, 2022, Meeting Summary," October 12, 2022, pages 2-3. (https://www.cisa.gov/sites/default/files/publications/CSAC_September_Quarterly_Meeting_Summary_Open_Session_1012_508.pdf)

112. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Memorandum for the Cybersecurity Advisory Committee Members," March 1, 2023, page 2. (https://www.cisa.gov/sites/default/files/2023-03/CSAC_September-Quarterly-Meeting-Recommendations_DIR-Response_2023-03-01_508_V2.pdf)

113. As defined by: U.S. Congress, "Department of Homeland Security Appropriations Bill, 2023," House Report 117-396. (https://www.congress.gov/117/crpt/hrpt396/CRPT-117hrpt396.pdf)

114. U.S. House Homeland Security Committee, "Garbarino, Swalwell Send Bipartisan Letter to CISA Director Easterly on New 'Systemically Important Entities' Office," April 27, 2023. (https://homeland.house.gov/2023/04/27/garbarino-swalwell-send-bipartisan-letter-to-cisa-director-easterly-on-new-systemically-important-entities-office)

115. National Security Agency, "NSA Cybersecurity Year in Review," 2022, page 9. (https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF)

116. Ibid., pages 9-10.

117. The Office of the Director of National Intelligence, "National Intelligence Strategy 2023," 2023. (https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf)

118. Ibid., page 11.

119. 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)

120. National Defense Authorization Act for Fiscal Year 2023, H.R. 7900, 117th Congress (2022), page 1,436. (https://www.congress.gov/117/bills/hr7900/BILLS-117hr7900pcs.pdf)

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

122. U.S. Senate Committee on Armed Services, "Joint Explanatory Statement to Accompany the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023," accessed September 8, 2023, page 349. (https://www.armed-services.senate.gov/imo/media/doc/fy23_ndaa_joint_explanatory_statement.pdf)

123. Consolidated Appropriations Act, 2023, Pub. L. 117-4743. (https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf)

124. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Fiscal Year 2024 Congressional Justification," accessed September 8, 2023, page 6. (https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf)

125. 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)

126. U.S. Senate Committee on Appropriations, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2023," March 2023, pages 57-58. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf)

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

128. U.S. Senate Committee on Appropriations, "Division F – Department of Homeland Security Appropriations Act, 2023," accessed September 8, 2023, page 55. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf)

129. The White House, "National Cybersecurity Strategy Implementation Plan," July 2023, page 18. (https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf)

130. The White House, "National Cybersecurity Strategy," March 1, 2023, page 11. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

131. The White House, "National Cybersecurity Strategy Implementation Plan," July 2023, page 17. (https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf)

132. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4120. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

133. Ibid., 134 Stat. 4092.

134. U.S. Senate Committee on Appropriations. "Division F – Department of Homeland Security Appropriations Act, 2023," page 57. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf)

135. 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)

136. U.S. Department of Defense, U.S. Cyber Command, "CYBERCOM's 'Under Advisement' to increase private sector partnerships, industry data-sharing in 2023," June 29, 2023. (https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat)

137. U.S. Department of Defense, "DOD Cyber Workforce Strategy Implementation Plan 2023-2027," July 13, 2023, pages 36-37. (https://media.defense.gov/2023/Aug/03/2003274088/-1/-1/1/2023-2027-DOD-CYBER-WORKFORCE-STRATEGY-IMPLEMENTATION-PLAN.PDF)

138. Joseph Clark, "Cybercom Commander Says Partnerships Are Key to Success in Challenging Strategic Environment," *U.S. Department of Defense*, May 2, 2023. (https://www.defense.gov/News/News-Stories/Article/Article/3381509/cybercom-commander-says-partnerships-are-key-to-success-in-challenging-strategi)

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

140. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4083. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

141. "The Evolution of Cyber: Newest Subordinate Unified Command is Nation's Joint Cyber Force," *U.S. Department of Defense, U.S. Cyber Command*, December 19, 2022. (https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe)

142. U.S. Department of Defense, Office of the Under Secretary of Defense, "United States Department of Defense Fiscal Year 2024 Budget Request," March 2023, page 10. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request.pdf)

143. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4086. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf); National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2028. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

144. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA Releases Malware Analysis Reports on Barracuda Backdoors," August 18, 2023. (https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors)

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

146. 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)

147. U.S. Cyber Command, "2023 Posture Statement of General Paul M. Nakasone," March 7, 2023. (https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone)

148. U.S. Department of Defense, "Fact Sheet: 2023 DOD Cyber Strategy," May 2023, page 2. (https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF)

149. National Defense Authorization Act for Fiscal Year 2020, Pub. L. 116-92, 133 Stat. 1747. (https://www.congress.gov/bill/116th-congress/senate-bill/1790/text)

150. U.S. Cyber Command, "2023 Posture Statement of General Paul M. Nakasone," March 7, 2023. (https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone)

151. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4119. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

152. Office of Senator Jacky Rosen, Press Release, "Rosen, Blackburn Introduce Bipartisan Bills to Strengthen Federal Response to Cyberattacks," March 21, 2023. (https://www.rosen.senate.gov/2023/03/21/rosen-blackburn-introduce-bipartisan-bills-to-strengthen-federal-response-to-cyberattacks)

153. National Defense Authorization Act for Fiscal Year 2024, S. 2226, 118th Congress (2023), page 750. (https://www.congress.gov/118/bills/s2226/BILLS-118s2226es.pdf)

154. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2028. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

155. Colin Demarest, "Troops need improved cyber education, US Army leaders say," *C4ISRNet*, August 17, 2023. (https://www.c4isrnet.com/cyber/2023/08/17/troops-need-improved-cyber-education-us-army-leaders-say)

156. U.S. Department of Defense, "DOD Cyber Workforce Strategy Implementation Plan 2023-2027," March 1, 2023. (https://media.defense.gov/2023/Aug/03/2003274088/-1/-1/1/2023-2027-DOD-CYBER-WORKFORCE-STRATEGY-IMPLEMENTATION-PLAN.PDF)

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

158. Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021. (https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity); The White House, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems)

159. Samantha Ravich and Mark Montgomery, "Harden the cybersecurity of US nuclear complex now," *C4ISRNet*, October 26, 2022. (https://www.c4isrnet.com/thought-leadership/2022/10/26/harden-the-cybersecurity-of-us-nuclear-complex-now); 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)

160. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4127. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

161. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136. Stat. 2899. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf)

162. Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Activities, 88 Federal Register 27832, May 3, 2023. (https://www.federalregister.gov/documents/2023/05/03/2023-09021/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities)

163. 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)

164. 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)

165. 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)

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

167. Jen Easterly and Deanne Criswell, "CISA and FEMA Partner to Provide $374.9 Million in Grants to Bolster State and Local Cybersecurity," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, August 8, 2023. (https://www.cisa.gov/news-events/news/cisa-and-fema-partner-provide-3749-million-grants-bolster-state-and-local-cybersecurity)

168. U.S. Department of Defense, Press Release, "Office of Strategic Capital, Small Business Administration to Sign Memorandum of Agreement," March 7, 2023. (https://www.defense.gov/News/Releases/Release/Article/3321429/office-of-strategic-capital-small-business-administration-to-sign-memorandum-of)

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

170. U.S. Government Accountability Office, "Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics," June 2023. (https://www.gao.gov/assets/gao-23-106080.pdf)

171. Better Cybercrime Metrics Act, Pub. L. 117-116. (https://www.congress.gov/117/plaws/publ116/PLAW-117publ116.pdf)

172. Cyber Peace Institute, Press Release, "CyberPeace Institute launches 'Humanitarian Cybersecurity Center (HCC)," February 27, 2023. (https://cyberpeaceinstitute.org/news/humanitarian-cybersecurity-center)

173. "SFOP0009762 Identify and Expose Kremlin Disinformation Networks," *Grants.gov*, June 16, 2023. (https://www.grants.gov/web/grants/view-opportunity.html?oppId=348773)

174. National Science Foundation, "Dear Colleague Letter: Workshop to Inform Development of the NSF Research on Research Security Program (RRSP)," June 29, 2023. (https://www.nsf.gov/pubs/2023/nsf23126/nsf23126.jsp)

175. 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)

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

177. Consolidated Appropriations Act, 2023, Pub. L. 117-4743, 136 Stat. 4664. (https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf)

178. The White House, "Nominations Sent to the Senate," July 25, 2023. (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/07/25/nominations-sent-to-the-senate-115)

179. Laura Bate and Mark Montgomery, "Workforce Development for the National Cyber Director," *CSC 2.0*, June 2022. (https://cybersolarium.org/csc-2-0-reports/workforce-development-agenda-for-the-national-cyber-director)

180. Office of the National Cyber Director, "National Cyber Workforce and Education Strategy," July 31, 2023, page 53. (https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf)

181. Ibid., page 43.

182. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 1956. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

183. Kiran A. Ahuja, "The AI in Government Act of 2020 – Artificial Intelligence Competencies," Office of Personnel and Management, July 6, 2023. (https://chcoc.gov/content/ai-government-act-2020-%E2%80%93-artificial-intelligence-competencies)

184. Office of the National Cyber Director, "National Cyber Workforce and Education Strategy," July 31, 2023, page 40. (https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf)

185. U.S. Senate Committee on Appropriations, "Division F – Department of Homeland Security Appropriations Act, 2023," pages 55-56. (https://www.appropriations.senate.gov/imo/media/doc/Division%20F%20-%20Homeland%20Statement%20FY23.pdf)

186. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Threats," January 2023. (https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf)

187. The White House, Press Release, "Biden-Harris Administration Launches New Efforts to Strengthen America's K-12 Schools' Cybersecurity," August 7, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/07/biden-harris-administration-launches-new-efforts-to-strengthen-americas-k-12-schools-cybersecurity)

188. Sundar Pichal, "Support for Cybersecurity Clinics Across the U.S.," *Google*, June 22, 2023. (https://blog.google/inside-google/message-ceo/commitment-cybersecurity-workforce); "About the Consortium," The Consortium of Cybersecurity Clinics, accessed September 8, 2023. (https://cybersecurityclinics.org/about)

189. Office of the National Cyber Director, "National Cyber Workforce and Education Strategy," July 31, 2023, page 18. (https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf)

190. Ibid., page 41.

191. Office of Personnel Management, "GS-2210: Information Technology Management Series," accessed September 8, 2023. (https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/0300/gs-2210-information-technology-management-series)

192. Jared Serbu, "DoD looks to expand Cyber Excepted Service, won't implement new SSR for IT workforce," *Federal News Network*, May 26, 2023. (https://federalnewsnetwork.com/federal-report/2023/05/dod-looks-to-expand-cyber-excepted-service-wont-implement-new-ssr-for-it-workforce)

193. National Science Foundation, "FY 2024 Budget Request to Congress," March 13, 2023, page 7. (https://nsf-gov-resources.nsf.gov/2023-03/NSF%20FY24%20CJ_Entire%20Rollup-revised.pdf?VersionId=piT6beLuOyugsHnEnBgrvdTknW8564PZ)

194. "Cyber Workforce Dashboard," Office of Personnel Management, accessed September 8, 2023. (https://www.opm.gov/data/data-products/cyber-workforce)

195. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1530. (https://www.congress.gov/bill/117th-congress/house-bill/4346)

196. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3904. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf)

197. U.S. Department of Defense, Press Release, "Defense Production Act Title III Presidential Determination for Printed Circuit Boards and Advanced Packaging Production Capability," March 27, 2023. (https://www.defense.gov/News/Releases/Release/Article/3342032/defense-production-act-title-iii-presidential-determination-for-printed-circuit)

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

199. U.S. Department of State, "Department of State Allocating $100 Million in FY 2023 for CHIPS Act Projects," March 14, 2023. (https://www.state.gov/department-of-state-allocating-100-million-in-fy-2023-for-chips-act-projects)

200. U.S. House of Representatives, Republican Homeland Security Committee, "Homeland Security Republicans Request Admin Briefing on Threats Posed by CCP to ICT Supply Chain," May 23, 2023. (https://homeland.house.gov/2023/05/23/homeland-security-republicans-request-admin-briefing-on-threats-posed-by-ccp-to-ict-supply-chain)

201. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1642. (https://www.congress.gov/bill/117th-congress/house-bill/4346); "Find Potential NSF Engines," U.S. National Science Foundation, accessed September 8, 2023. (https://new.nsf.gov/funding/initiatives/regional-innovation-engines/find-potential-nsf-engines)

202. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1581. (https://www.congress.gov/bill/117th-congress/house-bill/4346)

203. U.S. Department of Commerce, National Telecommunications and Information Administration, Press Release, "NTIA Requests Public Comment on CHIPS and Science Act Innovation Fund Implementation," December 12, 2022. (https://ntia.gov/press-release/2022/ntia-requests-public-comment-chips-and-science-act-innovation-fund)

204. 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); "Sector Risk Management Agencies," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed August 30, 2022. (https://www.cisa.gov/stopransomware/sector-risk-management-agencies)

205. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Fiscal Year 2024 Congressional Justification," March 2023, pages 7 and 343. (https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf)

206. U.S. Department of Commerce, National Institute of Standards and Technology, Press Release "Biden-Harris Administration Awards $20 Million to Make Domestic Supply Chains More Resilient," June 9, 2023. (https://www.nist.gov/news-events/news/2023/06/biden-harris-administration-awards-20-million-make-domestic-supply-chains)

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

208. Ibid., Stat. 429.

209. Gina Raimondo and Alan Davidson, "Annual Report on the Status of Spectrum Repurposing and Other Initiatives," *U.S. Department of Commerce*, March 2023, page 5. (https://ntia.gov/sites/default/files/publications/annual_spectrum_repurposing_initiatives_report_final.pdf)

210. U.S. Department of State, "Digital Connectivity and Cybersecurity Partnership," October 2021. (https://www.state.gov/wp-content/uploads/2021/11/2021-023h-CD-DCCP-One-Pager-10292021-Accesssible-11012021.pdf)

211. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1372. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

212. American History and Civics National Academies received $3 million and American Civics National Activities received $20 million in a competitive grant program. See: U.S. Senate Committee on Appropriations, "Division H - Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2023," page 236. (https://www.appropriations.senate.gov/imo/media/doc/Division%20H%20-%20LHHS%20Statement%20FY23.pdf)

213. American History and Civics National Activities programs are defined under this heading. See: U.S. Congress, "Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Bill, 2023," House Report 117-403, page 260. (https://www.congress.gov/117/crpt/hrpt403/CRPT-117hrpt403.pdf)

214. U.S. House Committee on Appropriations, "Division H, Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2022," page 148. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-H_Part2.pdf)

215. The White House, "Budget of the U.S. Government Fiscal Year 2024," March 2023, page 38. (https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf)

216. "SFOP0009762 Identify and Expose Kremlin Disinformation Networks," *Grants.gov*, June 16, 2023. (https://www.grants.gov/web/grants/view-opportunity.html?oppId=348773)

217. Gary Price, "NSF Awards Five $5 Million Grant to Help Older Adults Spot Online Scams, Disinformation," *Library of Journal*, October 6, 2022. (https://www.infodocket.com/2022/10/06/nsf-awards-five-5-million-grant-to-help-older-adults-spot-online-scams-disinformation)

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

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

220. Office of Senator Maggie Hassan, Press Release, "PASSED THE SENATE: Bill Cosponsored by Senator Hassan to Close Foreign Lobbying Loophole," June 28, 2023. (https://www.hassan.senate.gov/news/press-releases/passed-the-senate-bill-cosponsored-by-senator-hassan-to-close-foreign-lobbying-loophole)

221. Joseph Menn, "Twitter removes labels from state-controlled media, helping propaganda," *The Washington Post,* April 21, 2023. (https://www.washingtonpost.com/technology/2023/04/21/twitter-russia-china-state-media-propaganda)

About the Authors

Jiwon Ma is a program analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. Before joining FDD, she was the editor-in-chief of the Journal of International Affairs at Columbia University. She has contributed to cybersecurity reports published by the School of Public and International Affairs at Columbia University and by the Belfer Center for Science and International Affairs. Jiwon received a Master of International Affairs from Columbia University's School of International and Public Affairs and a BA in global studies from Lesley University.

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

ACKNOWLEDGEMENTS

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

Cover Photo: Representative Mike Gallagher and Senator Angus King speak at event hosted at the Foundation for Defense of Democracies on September 21, 2022. (Photo by Ralph Alswang/copyright FDD)

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

Michael "Mike" J. Gallagher, 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

Thomas A. "Tom" Fanning, Executive Chairman of Southern Company

Chris Inglis, Former U.S. National Cyber Director

James R. "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

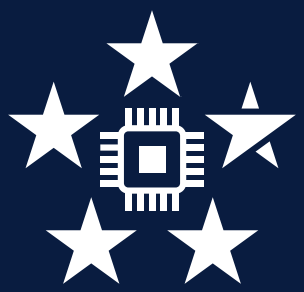
Benjamin E. "Ben" Sasse, Former U.S. Senator for Nebraska

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

Partners

FDD

McCRARY INSTITUTE
FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission