CSC 2.0

September 2022

2022 Annual Report on Implementation

Jiwon Ma
Mark Montgomery

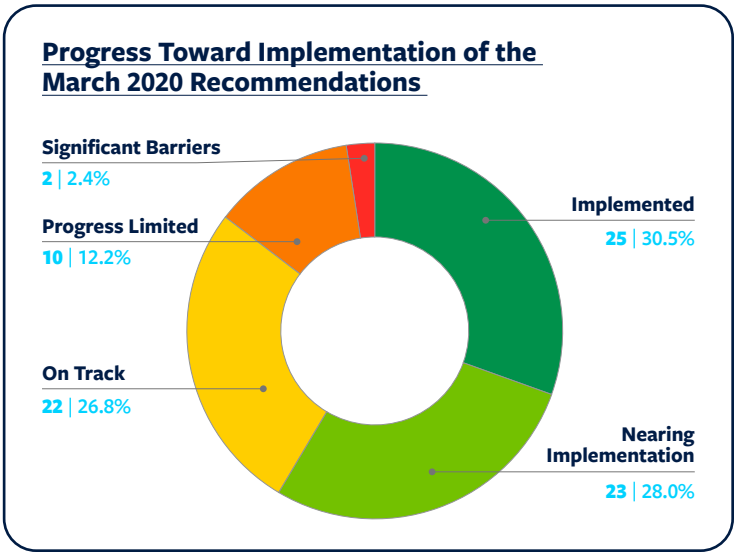
Table of Contents

Executive Summary

The past two years have been witness to significant improvements in U.S. cybersecurity. Critical legislation has broken loose from long-standing jurisdictional conflicts to become law. Congress passed the Cyber Incident Reporting Act, which requires critical infrastructure companies to report cyberattacks and ransomware incidents. Lawmakers have increased funding for government cybersecurity efforts, particularly at the country's primary cybersecurity agency, the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security, whose budget has grown by more than 25 percent, from $2 billion for FY20 appropriation[1] to $2.59 billion for FY22 appropriation.[2] Even more funding is expected in FY23.[3] The White House now has a national cyber director (NCD) to lead the coordination of cybersecurity strategy and policy implementation across the government. The State Department has a bureau and a nominated ambassador charged with leading America's international engagement on cyberspace challenges. And the executive branch has taken other important actions (based on new legislation), such as the establishment of the Joint Cyber Defense Collaborative at CISA.

Collectively, these changes will help deter malign actors in cyberspace and shore up U.S. defenses at home. They will also make digital interactions safer for stakeholders across industry and around the world. Most importantly, these changes will help to protect every American who uses the internet for work, study, or staying connected with loved ones. However, this progress cannot be the culmination of the U.S. government's focus on cybersecurity; it must be the prelude to even further changes.

Congress created the U.S. Cyberspace Solarium Commission (CSC) 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. The Commission's original report in March 2020 had 82 recommendations. Of these, nearly 60 percent are fully implemented or nearing implementation, and more than 25 percent are on track to implementation.



However, implementation is not the same as success. Lasting improvements in national cyber resilience will take sustained attention, investment, and agility to address the ever-shifting threat landscape. Accordingly, this assessment details both the progress of the Commission's original work as well as the work of the non-profit CSC 2.0 project that has accepted the baton in the long race to secure cyberspace. Even as we issue this progress report, we know that assessing implementation is not enough. We urge readers to consider this report as a mid-course check, laying a path for the many stakeholders in government and industry charged with a task that we cannot afford to fail — protecting our national cybersecurity.

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

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

Commission Background

Congress established the U.S. Cyberspace Solarium Commission in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA) to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."[4] To meet its mandate, the CSC produced a final report, published in March 2020, outlining a strategic approach and 82 recommendations for the U.S. government. In the months following, commissioners and staff produced legislative proposals (where appropriate) to support its recommendations and worked with relevant committees in the House and Senate to implement many of the Commission's original recommendations.

In addition, the Commission issued six white papers with new and updated recommendations. They addressed lessons on cybersecurity from the pandemic, details on the recommendation to establish the Office of the National Cyber Director (ONCD), a framework for a cybersecurity workforce development strategy, proposals on how to secure America's information and communications technology (ICT) supply chains, and recommendations to counter malign foreign disinformation. The Commission also published a transition book in January 2021, highlighting specific priorities and executive branch actions for the incoming Biden-Harris administration.

Transition to CSC 2.0 and Future Plans

In August 2021, the Commission published its first Annual Report on Implementation, highlighting the fact that implementation of the Commission's recommendations is only the first step towards successful long-term improvements in U.S. cybersecurity.[5] That report — and this one — considers a recommendation to be implemented if Congress has codified it in law, if the executive branch has begun work towards the goal, or if other definitive signs indicate that work is or will soon be underway. However, driving lasting change beyond this initiation of work takes investment and careful stewardship over time. This long-term attention was not a viable prospect for the original CSC, which was subject to a congressionally directed sunset date at the end of 2021.[6]

With the goal of continuing implementation and supporting long-term success, the CSC 2.0 project will continue ongoing work, like monitoring and assessing the status of recommendation implementation.

As the CSC reached the planned end of its mandate, the commissioners agreed to continue the work under the auspices of the CSC 2.0 project. With the goal of continuing implementation and supporting long-term success, the CSC 2.0 project will continue ongoing work, like monitoring and assessing the status of recommendation implementation. CSC 2.0 will also continue research and analysis on outstanding recommendations, ensuring that policymakers have detailed, up-to-date information. As such, this second annual assessment reviews the implementation of CSC recommendations over the course of the previous year to evaluate progress and highlight remaining gaps as policymakers implement and execute recommendations.[7] Many of the Commission's key recommendations have been enacted in legislation, but there is still more work to be done to meet the urgent challenges facing our nation.

Beyond preserving and maintaining the existing body of work, the CSC 2.0 project is also undertaking novel research. Cybersecurity is not a stationary target. The priorities the Commission identified in 2020 have developed and changed in the intervening years, and new issues have come to the forefront. The CSC 2.0 project will research, analyze, and develop policy proposals. In fact, as discussed in the assessment that follows, this work is already underway.

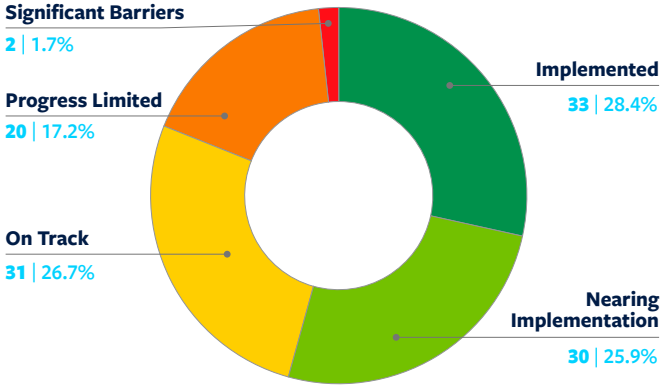
Finally, as a practical matter, CSC 2.0 will also provide a digital home to the Commission's work: www.cybersolarium.org. This shift ensures that reports, legislative proposals, assessments, and other content remain publicly available once the Commission's original website, www.solarium.gov, is retired.

Evaluating Progress

While much work is yet required to fully implement the CSC's recommendations, an interim review of progress shows that cybersecurity leaders throughout the government have taken significant steps. 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 attacks of significant consequence in cyberspace. This section outlines the methodology used in this assessment.

The FY21 NDAA added to the CSC's mandate by including the charge to review the implementation of the CSC's recommendations and provide annual updates.[8] This report is the second annual implementation review responding to that mandate. For the purposes of this assessment, indicators of progress toward implementation of Commission recommendations are varied but appear most frequently in authorizing legislation, appropriations, and executive branch policy and actions.

Progress Toward Implementation of All 116 Recommendations



Authorizing Legislation: In July 2020, the Commission staff published a package of 54 legislative proposals,[9] many of which served as the starting point for legislation later included in the FY21 NDAA. Indeed, the FY21 NDAA included a historic number of cybersecurity provisions, 27 of which represent the implementation of 25 different CSC recommendations. The FY22 NDAA included an additional 12 recommendations. Additional legislation, most notably the Infrastructure Investment and Jobs Act (six recommendations) and the CHIPS and Science Act (11 recommendations), accounted for more implemented proposals. After the publication of the March 2020 report and accompanying legislative proposals, the Commission also published proposals to accompany its white papers. The CSC 2.0 project has similarly published model legislative text to demonstrate how policymakers can implement recommendations identified in its research.[10] These proposals are mentioned in brief at the end of this assessment.

Appropriations: The CSC's congressional commissioners highlighted 19 funding priorities during the FY21 appropriations cycle,[11] 42 for FY22,[12] and 35 in FY23. The growth in the latter two years reflects the historic legislative progress on cybersecurity. The growing cybersecurity mandates, especially at CISA, warrant increased funding. Congressional appropriators have recognized this need, and 29 of the priorities highlighted by commissioners were funded or addressed in the Consolidated Appropriations Act, 2021,[13] the Infrastructure Investment and Jobs Act,[14] the Consolidated Appropriations Act, 2022,[15] and the Joint Explanatory Statements included with these bills. The CSC's congressional commissioners wrote letters to their appropriations colleagues highlighting for the FY23 cycle those priorities not already included or funded in the FY21 or FY22 appropriations cycles, as well as those newly authorized in 2022.

U.S. President Joe Biden is joined by Vice President Kamala Harris, Office of Management and Budget Acting Director Shalanda Young, and congressional leaders as he signs the Consolidated Appropriations Act on March 15, 2022. (Nicholas Kamm/AFP via Getty Images)

Executive Orders and Policy: In its "Transition Book for the Incoming Biden Administration," the CSC outlined three priority areas of focus for the first hundred days and an additional six priority areas for attention beyond one hundred days. Collectively, these areas represent 30 individual activities and address many of the non-legislative recommendations of the March 2020 CSC report. As the administration approaches its midway point, many of those actions are underway.

Other Actions: In some instances, indicators of progress fall outside the activities outlined above, or government leaders are carrying the actions out in tandem with, or in anticipation of, official legislation or policy. Furthermore, the Commission's recommendations were not made in a vacuum. They were the result of hundreds of conversations between commissioners, staff, government representatives, subject matter experts, and many others. Consequently, many actions undertaken in cyberspace policy over the course of the past year both shaped, and were shaped by, Commission recommendations. Even legislation that started with a CSC-provided template never came out exactly the way the Commission envisioned, as edits from lawmakers and their staff and feedback from the executive branch would alter, and almost always improve, the legislative text. The same is true for executive branch actions. Recognizing this dynamic, this assessment considers actions taken that align with CSC recommendations to be indicators of progress in implementing them, with the full appreciation that commendation for success in these — and all — cases is due to the hard work of cybersecurity and policy professionals in government and beyond. While these activities have not always been made public, the assessment below accounts for them to the extent possible.

Over its tenure, the Commission focused heavily on developing and shaping recommendations that had a clear path to implementation. And yet, the commissioners also recognized that limitations based on current circumstances should not inhibit its endorsement of ideas that could lead to dramatic improvement. Thus, the commissioners and staff anticipated, even as they were drafting certain recommendations, that some would face significant barriers to implementation. Indeed, the assessment below identifies two recommendations (marked in red) that are unlikely to overcome current barriers to implementation but that remain valid proposals, in the Commission's view. Recommendations can sometimes regress if expected progress is not successfully completed.

In the following sections, progress toward implementation of each recommendation is given a single score 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 presents 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**	**Status**	**Assessment**
1.1	Issue an Updated National Cyber Strategy	In Progress	
1.1.1	Develop a Multitiered Signaling Strategy	Executive Action Required	
1.1.2	Promulgate a New Declaratory Policy	Executive Action Required	
1.2	Create House Permanent Select and Senate Select Committees on Cybersecurity	Faces Significant Barriers to Implementation	
1.2.1	Re-establish the Office of Technology Assessment	GAO and CRS Funded for Tasking	
1.3	Establish a National Cyber Director Position	Legislation Passed in FY21 NDAA; NCD Nominated and Confirmed	
1.4	Strengthen the Cybersecurity and Infrastructure Security Agency	Legislation Passed in FY21 NDAA; Appropriations in FY21 and FY22	
1.4.1	Codify and Strengthen the Cyber Threat Intelligence Integration Center	Legislation Passed; Administration Re-established CTIIC	
1.4.2	Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force	Appropriations Proposed	
1.5	Diversify and Strengthen the Federal Cyberspace Workforce	Partial Implementation via Legislation Passed in FY21 NDAA; Further Legislation and Appropriations Required	
1.5.1	Improve Cyber-Oriented Education	Increased Appropriations Required	

Recommendation 1.1 – Issue an Updated National Cyber Strategy: On December 20, 2021, CSC co-chairs Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI) sent a letter to President Joe Biden, urging the issuance of a national cyber strategy in order to bolster national deterrence through clear international signaling.[16] On two separate occasions in 2021, administration officials indicated that a national cyber strategy is underway.[17] In May of this year, the national security advisor delegated to the ONCD to draft the forthcoming national cyber strategy.[18] Once the strategy is issued, this recommendation will be considered implemented. In order to be fully successful once implemented, the strategy should designate lines of effort and clarify priorities, and in doing so, draw on concepts including layered cyber deterrence, international engagement, resilience, public-private collaboration, and defending forward.

Recommendation 1.1.1 – Develop a Multitiered Signaling Strategy: Executive action that demonstrates an intention towards clear signaling in cyberspace is clearly ongoing. For example, the June 2021 meeting with Russian President Vladimir Putin[19] and the international condemnation of the Russian government for disabling satellite internet in Ukraine in February 2022[20] both serve the purpose of clarifying U.S. expectations in cyberspace. Signaling about actions in cyberspace must continue to emphasize both cyber and non-cyber tools. While some manifestations of the implementation of this recommendation may take place out of public view, full implementation of this recommendation will require a publicly articulated strategy to communicate U.S. goals and intent in cyberspace.

Recommendation 1.1.2 – Promulgate a New Declaratory Policy: The first step towards implementation of this recommendation will be the publication of a national cyber strategy or similar public document that declares that the United States will impose cyber and/or non-cyber costs against adversary campaigns, including those that fall below the use-of-force threshold. Following the Russian invasion of Ukraine, the Biden administration has sought to deter Russian retaliation in cyberspace (for instance, through CISA's ongoing "Shields Up" campaign). These efforts help reinforce U.S. red lines in cyberspace, strengthening deterrence. To maintain deterrence, the United States must reinforce this strategy with clear and consistent action. On December 20, 2021, Senator King and Representative Gallagher sent a letter to President Biden urging the issuance of a national cyber strategy, which would serve as the implementation of this recommendation.[21]

Recommendation 1.2 – Create House Permanent Select and Senate Select Committees on Cybersecurity: Continuing into a second year, the Commission expected and encountered significant pushback against this recommendation, which is one of the two that face known significant barriers to implementation. However, the recommendation has been drafted into legislative language and stands ready should a future emergency create the political impetus needed to overcome existing barriers.

Recommendation 1.2.1 – Re-establish the Office of Technology Assessment: Although Congress has authorized the Office of Technology Assessment (OTA), it is currently unfunded. Last year, congressional appropriators indicated that strengthening technological expertise in the Government Accountability Office (GAO) and the Congressional Research Service is a preferred alternative to re-establishing the Office of Technology Assessment.[22] The Joint Explanatory Statement to the Consolidated Appropriations Act, 2022 includes language very similar to the prior year's and provided no funding for OTA, but continued funding for GAO and CRS efforts.[23] CSC's congressional commissioners did repeat their recommendation for separate funding for the OTA out of concern that some functions were going unmet.[24] In addition to the reintroduction of the 2019 Office of Technology Assessment Improvement and Enhancement Act,[25] GAO and CRS's increased attention has addressed the issue initially surfaced by the Commission and may resolve the issue in the long term.

Recommendation 1.3 – Establish a National Cyber Director Position: In 2021, Congress established the NCD position in Section 1752 of the FY21 NDAA, and on June 17 of that year, the Senate confirmed Chris Inglis as the first director to serve in the post.[26] While these steps reflect the full implementation of this recommendation, successful execution of the position will require personnel and resources suited to the task. The Commission had proposed an expanded hiring authority for the ONCD.[27] A main element of this proposal, which allows the NCD to accept detailees from other departments and agencies on a non-reimbursable basis, were incorporated into the final FY22 NDAA.[28] Meanwhile, the Infrastructure Investment and Jobs Act, signed into law on November 15, 2021, appropriated $21 million for salaries and expenses for the ONCD.[29] This funding significantly accelerated the assembly of the office, which continues to grow towards full staffing. However, that initial appropriation remains available only until September 30, 2022, meaning that additional appropriations will be needed to allow the office to continue to grow into the fiscal year 2023, as the appropriations bill for FY22 noted.[30] This will need to be carried forward into FY23 if the ONCD is to continue to be successful, and the president's budget request for FY23 puts the office on the right track to do so.[31] More generally, the White House must continue to empower the role, ensuring that it is positioned to provide whole-of-government coordination on cyber issues by implementing policies consistent with the CSC's recommendations for the NCD.

Recommendation 1.4 – Strengthen the Cybersecurity and Infrastructure Security Agency: This recommendation was largely implemented through Sections 1705, 1718, 1745, and 9001 of the FY21 NDAA, and further efforts including incident response planning and vulnerability reduction were implemented in the 2021 Executive Order on Improving the Nation's Cybersecurity.[32] The remaining legislative element of this recommendation, establishing a five-year term for the CISA director, was included as Section 1536 in the House version of the FY22 NDAA. However, it was not included in the Senate's version and was similarly omitted from the final FY22 NDAA.[33] Beyond authorizing legislation, the past year has seen monumental progress for CISA's funding. For FY22, the CSC's congressional commissioners recommended an increase of $400 million to the budget to allow for growth at

CISA.[34] Subsequently, the FY22 spending bill passed in March made historic increases to CISA funding, increasing the budget by $568,680,000 over the prior year's spending.[35] Notably, though, CISA will need to grow its staff and programming rapidly to meet its new mandate and expanded resources. Doing so will require significant improvements to basic business processes like human resources and procurement. However, the president's budget request for FY22 proposed adding only a single full-time-equivalent position and $1 million to the CISA Office of the Chief Human Capital Officer,[36] an increase that falls drastically short of the human resources support needed to accommodate CISA's rapid growth amid an already challenging cybersecurity hiring environment. The CSC's congressional commissioners previously recommended bolstering appropriations for CISA's Mission Support/Management and Business Activities funding line.[37] Both the president's budget request and congressional appropriations should account for this need in future funding plans.

Recommendation 1.4.1 – Codify and Strengthen the Cyber Threat Intelligence Integration Center: Prior to the end of the CSC's congressional mandate, Commission staff drafted proposed legislation requiring a report on the potential for improved federal all-source intelligence integration related to cyber incidents and threats. The Intelligence Authorization Act, passed as part of the FY22 spending omnibus, includes a provision that calls for a "report on the potential to strengthen all-source intelligence integration relating to foreign cyber threats."[38] This partially meets the intent of this recommendation. More critically, the Biden administration re-established the Cyber Threat Intelligence Integration Center, although it does not yet appear to be at the size recommended by the Commission. Full implementation will require action in response to the mandated report.

Recommendation 1.4.2 – Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force: The FBI draws on a network of field offices and cyber task forces to both protect national security and enforce federal laws. Additionally, the National Cyber Investigative Joint Task Force (NCIJTF) works across the federal government to coordinate and integrate information from different departments and agencies to support cyber threat investigations. These elements are critical to protecting domestic cybersecurity but require additional resources to be maximally effective. In letters to appropriators in both FY21[39] and FY22,[40] the CSC's congressional commissioners recommended an increase in funding for the FBI's cyber mission (as distinct from its own organizational cybersecurity efforts) and the NCIJTF. The Senate majority's proposed funding bill for FY22 highlighted the importance of these efforts but directed the Department of Justice "to maintain its cybersecurity posture at no less than the fiscal year 2021 enacted level to defend against and respond to current and emerging threats,"[41] with no increase in funding specified. The House version of the bill, however, included an increase of $40,000,000 for "the FBI's efforts to deter, investigate, and pursue cyberthreats and cybercrime,"[42] which aligned with an increase in the president's budget request.[43] Congress, however, ultimately did not include this funding in the final FY22 appropriations bill.[44] The president's budget request for FY23, however, includes a $52 million increase for the FBI's cyber mission that, if met, would be a major step towards implementation of this recommendation.[45] The recommendation would be fully implemented once the FBI uses the funds to bolster the NCIJTF and expand capability and personnel for investigative, analytical, and technical work.

Recommendation 1.5 – Diversify and Strengthen the Federal Cyberspace Workforce: As noted in last year's assessment, the FY21 NDAA partially implemented this recommendation.[46] Since that time, Congress considered numerous further elements of this recommendation in legislation and appropriations, with some provisions making it and some failing. The passage of the CHIPS and Science Act calls for strengthening the federal cyber Scholarship for Service program at the National Science Foundation and amends the Cybersecurity Enhancement Act of 2014 to add cybersecurity-related fields, such as artificial intelligence, quantum computing, and aerospace to the Scholarship for Service program.[47] Senators Maggie Hassan (D-NH) and John Cornyn (R-TX) introduced the Federal Cybersecurity Workforce Expansion Act, which would have created a cybersecurity-focused upskilling pilot program for service members transitioning to civilian life and would have authorized a cybersecurity apprenticeship program at CISA, expressly permitting the use of an apprenticeship intermediary to support the process.[48] Congress did not include these provisions in the FY22 NDAA but did include a provision (Section 1506) calling for the secretary of defense to assess current and future educational requirements for both military and civilian personnel.[49] Separately, in June, President Biden signed the Federal Rotational Cyber Workforce Program Act into law. The intent of this rotational program is to attract, retain, and provide additional professional experiences to the federal cyber workforce.[50] Beyond authorizing legislation, funding considerations are a recurring challenge in cybersecurity workforce development, where the scalability of efforts is critically important. In particular, the CSC has recommended additional investments in the CyberCorps: Scholarship for Service program, and CSC's congressional commissioners recommended a $20 million increase in FY21 appropriations and again in FY22.[51] The program has received increased funding, but not to the degree recommended.[52] The president's budget request for FY23 would implement a more significant increase, to $75 million, which comes far closer to the Commission's recommendation.[53] Similarly, the Regional Alliances and Multistakeholder Partnerships program established in FY21 NDAA Section 9401[54] requires additional funding to be fully effective. The president's

budget request for FY22 made no specific funding request for this cybersecurity workforce program and requested only minimal funding increases to the budget for the cybersecurity and privacy teams within the National Institute of Standards and Technology (NIST) supporting the effort.[55] The FY22 omnibus spending bill designated only $500,000 for this effort.[56] The president's budget request for FY23 recommends $7 million,[57] which is less than the Congressional Budget Office had indicated would be needed[58] but still a valuable start for the program. Finally, the ONCD is assuming a leadership role on federal cyber workforce issues, convening a White House summit in mid-July.[59] At the summit, Director Inglis announced that his office is leading the creation of a cyber education and workforce strategy.[60] The Departments of Commerce and Labor also announced a cyber apprenticeship sprint to expand the existing apprenticeship programs.[61] Earlier this year, CSC 2.0 published a memo outlining recommendations for the ONCD and Congress.[62] While not included as a separate section of this assessment, positive movement towards implementing these recommendations is included in the assessment of the Commission's original federal cyber workforce recommendation. Considering the summation of these actions, this recommendation is considered partially implemented, but cybersecurity workforce development must be a long-term effort that continues far past the specific recommendations made here.

Recommendation 1.5.1 – Improve Cyber-Oriented Education: Subsequent to the implementation of this recommendation through the codification of the Cybersecurity Education and Training Assistance Program in Section 1719 of the FY21 NDAA, the Commission advocated for increased and consistent funding for this grant program, which provides curricula and training to K-12 teachers. As the executive branch has indicated, the key to supporting this program is conducting outreach and support at scale, which probably requires close to $20 million per year.[63] However, the president's budget request for FY23 suggests cutting the funding that had previously been allotted to this program and relocating K-12 cybersecurity education efforts to the National Science Foundation[64] This move would both undermine existing work funded by CISA and overwhelm successful programming at the Foundation. This cut appears unlikely to make its way into the FY23 appropriations, as the Senate majority version of the bill rejected the change, and the House version called to increase funding to $6.8 million.[65] Nevertheless, the lack of clarity and stability inhibits the long-term growth of this program.

Pillar 2: Strengthen Norms and Non-military Tools

Strengthen Norms and Non-military Tools			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
2.1	Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State	Implemented via Executive Action; Legislation and Appropriations Required	
2.1.1	Strengthen Norms of Responsible State Behavior in Cyberspace	Executive Actions Taken	
2.1.2	Engage Actively and Effectively in Forums Setting International ICT Standards	Legislation Passed; Appropriations Required	
2.1.3	Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance	Legislation Proposed; Appropriations Required	
2.1.4	Improve International Tools for Law Enforcement Activities in Cyberspace	Executive Action Taken; Funding Appropriated	
2.1.5	Leverage Sanctions and Trade Enforcement Actions	Legislation Proposed; Executive Action Taken	
2.1.6	Improve Attribution Analysis and the Attribution-Decision Rubric	Executive Actions Taken	
2.1.7	Reinvigorate Efforts to Develop Cyber Confidence-Building Measures	Executive Actions Taken	

Recommendation 2.1 – Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State: As of publication, the Cyber Diplomacy Act has not yet been passed. However, the State Department opened its Bureau of Cyberspace and Digital Policy on April 4, 2022, which an ambassador-at-large will lead. The president has nominated an official who is awaiting Senate confirmation. This new bureau will bypass prior stove-piped structures to drive the prioritization of key international cyber policy issues. The Senate is considering ways to pass the Cyber Diplomacy Act so that the new bureau is permanently established and can be resourced appropriately for expansion and to execute its mandate successfully. In addition to basic operations, the bureau will also require funding to pursue specific lines of effort, like engaging with the private sector to promote participation and communication around standards-setting bodies, supporting capacity building projects, combating cybercrime, and other critical activities. The CSC's congressional commissioners have continued to advocate for this appropriations priority in FY23.

Recommendation 2.1.1 – Strengthen Norms of Responsible State Behavior in Cyberspace: Rather than any single action, implementation of this recommendation will take a broad shift in approach towards international cyberspace policy, and recent actions are indicative of progress. For example, the 30-nation summit to address ransomware in October of 2021 demonstrates a proactive approach toward working with the international community to reinforce existing norms around combating cybercrime.[66] Similarly, the joint attribution in May 2022 of Russian government actions to disable Ukrainian satellite internet helps to reinforce norms around critical infrastructure.[67] In NATO's recently released 2022 Strategic Concept, the alliance reaffirmed its stance that a cyberattack against one of its member states could potentially trigger Article 5 of the North Atlantic Treaty, meaning that a cyberattack against one of its member states could be considered an attack against the alliance as a whole.[68] The 2022 National Cyber Strategy should reflect this emphasis, clearly prioritizing enforcement of responsible state behavior in cyberspace through a collective approach with the international community. Implementing this recommendation will be more successful if the new Bureau of Cyberspace and Digital Policy is adequately resourced through FY23 appropriations.

Recommendation 2.1.2 – Engage Actively and Effectively in Forums Setting International ICT Standards: The passage of the CHIPS and Science Act partially implements this recommendation. Section 10245 creates technical standards education and training resources, improves the ability to partner with the private sector on standards for emerging technologies, drives greater coordination across the federal government on participation in international technical standards bodies, and provides education and workforce development efforts to promote participation in international technical standards bodies.[69] However, a critical factor in the long-term success of this recommendation stems from NIST's capacity to promote the development of and coordination around international standards. In large part, this is a function of growth in the cybersecurity and privacy program area. Despite the clear need for growth in this area, the FY22 budget submission to Congress reflected only a six percent increase over FY21 enacted spending, from $77.5 million to $81.9 million, though the administration asked for a 45 percent increase to NIST's budget overall. The FY22 request also included a $2.35 million increase for the Standards Coordination and Special Programs portfolio, which supports international standards development, but overall, these increases are dwarfed by spending on other NIST priorities.[70] The FY22 omnibus appropriations bill provided a minimal — $1.5 million — increase above the request for cybersecurity and privacy, an amount that clearly falls short of the increasing priority of international technical standards.[71] The president's FY23 budget does request a 20 percent ($18 million) increase for this funding priority, but after so many years of underfunding NIST's cybersecurity and privacy mission, this increase is insufficient.[72] The CSC's congressional commissioners emphasized this critical funding need in an April 2022 letter to appropriators.

Recommendation 2.1.3 – Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance: Implementation of this recommendation will require legislation and appropriations. Currently, cybersecurity capacity building efforts are split across a number of different funds, each with its own priorities and restrictions. In 2021, CSC staff provided relevant committee staff with a legislative proposal that would consolidate international cybersecurity capacity building efforts under a single fund. In the interim, the CSC's congressional commissioners have and will continue to recommend increases to international development funds that support international capacity building. Encouragingly, the FY22 House consolidated appropriations report included specific increases in the funds for Assistance for Europe, Eurasia, and Central Asia and International Narcotics Control and Law Enforcement.[73] It also recommended that "the [State] Department expand efforts to hire experienced personnel to support cybersecurity capacity building," which would greatly expand the Department's impact on global cybersecurity.[74] However, the final bill did not include these provisions. The president's budget request for FY23 does appear to consolidate several related areas of capacity building in the Economic Support Fund under the new Bureau for Cyberspace and Digital Policy, but that consolidates programs already in one fund rather than consolidating efforts across funds.[75] Additionally, the president's budget request for FY23 also provides $682 million for Ukraine to counter Russian influence, including cybersecurity issues and disinformation, an increase of $219 million above the 2021 enacted level.[76]

Recommendation 2.1.4 – Improve International Tools for Law Enforcement Activities in Cyberspace: Implementation of this recommendation rests on two primary elements to strengthen international law enforcement. The first is a legislative change granting subpoena authority to the Office of International Affairs at the Department of Justice. This proposal, which Commission staff drafted, would be a valuable tool to expedite the processing of requests under mutual legal assistance treaties. The second element of this recommendation would require increased funding to expand the number of Cyber Assistant Legal Attachés (ALATs). As of publication, the number of ALATs has increased from 6 to 16 internationally.[77] The CSC's congressional commissioners recommended an increase in appropriations for this program. While the appropriators did not grant a specific increase, the House version of the FY22 Consolidated Appropriations Act did note strong support for the program and encouraged "the FBI to consider increasing funding for the Cyber ALAT program."[78] If funded, the significant increase requested in the FY23 president's budget for the FBI's cyber mission could be critical in fully implementing this recommendation.[79]

Recommendation 2.1.5 – Leverage Sanctions and Trade Enforcement Actions: The Commission recommended the codification of Executive Order 13848 as a means of improving enforcement norms of responsible state behavior in cyberspace.[80] However, this recommendation could also be implemented through executive branch action. For example, the administration's use of sanctions against the Russia-based darknet market, Hydra, as part of an internationally coordinated effort to disrupt cybercriminals' activities and cybercrime services demonstrates a willingness to use these tools.[81] Similarly, recent sanctions against Russian technology companies and cyber actors[82] supporting Russia's efforts to invade Ukraine make progress towards the overall goal of this recommendation. The scale and severity of sanctions against the Russian government and leaders in the spring of 2022 demonstrate the executive branch's willingness to use sanctions tools to protect norms of responsible state behavior in general.[83] While not specific to cybersecurity, this change has created an environment where this recommendation is more likely to be implemented effectively. Additional legislative and executive actions have been taken to further advance this recommendation's goals. For instance, the House version of the FY23 NDAA emphasizes the need to empower U.S. banking institutions to address modern financial threats. Section 5415 notes that the Financial Crimes Enforcement Network may require domestic financial institutions and agencies to take "special measures" to address money laundering and terrorist financing activities "to bring pressure on those that pose money laundering threats." The provision specifically identifies ransomware attacks perpetrated by Chinese and other malign foreign actors as a focus to combat modern financial crime. These special measures include prohibiting or imposing certain conditions upon transmittals of funds. In addition, the Department of Justice's Strategic Plan for the fiscal years 2022 through 2026 lists combating ransomware attacks and other cyber threats as one of the agency's main priorities and sets actionable goals to enhance its effectiveness in addressing ransomware attacks by September 30, 2023.[84]

Recommendation 2.1.6 – Improve Attribution Analysis and the Attribution-Decision Rubric: This recommendation seeks to streamline the attribution of cyberattacks through two elements. The Cyber Incident Data and Analysis Working Group would convene to respond to an emerging incident to coordinate attribution, and the Cyber Incident Attribution and Analysis Decision Rubric provides clear guidance on available responses to cyberattacks given a particular level of confidence in attribution. Both elements require executive action for implementation. The creation of these, or similar, tools may not be made public, even if implemented, but the speed of attribution has improved in recent years. For example, last year, the United States acted in concert with its EU, NATO, and Five Eyes allies to jointly attribute a disruptive and reckless attack on Microsoft's Exchange servers to China's Ministry of State Security.[85] While statements came nearly four months after the incident, the ability to pull together such an effort represents a commendable step in multilateral engagement on cybersecurity.[86] Governments were notably quicker in their subsequent joint attribution of Russian government hacking in Ukraine in February 2022.[87] Within just three days of a distributed denial-of-service (DDoS) attack against the Ukrainian Ministry of Defense, U.S. Deputy National Security Advisor Anne Neuberger accused Russia of perpetrating the attack.[88] The British government concurred.[89] Subsequently, CISA released an advisory noting the indicators of compromise of the associated attack.[90] The speedy attribution capabilities between the United States and its allies show the potential of this approach.

Recommendation 2.1.7 – Reinvigorate Efforts to Develop Cyber Confidence-Building Measures: Confidence-building measures promote stability and strengthen norms in cyberspace. Implementation requires executive action, and recent U.S. engagement internationally indicates progress towards implementing this recommendation. For example, President Biden's very prominent articulation[91] of the seriousness with which the U.S. government views cyberattacks against the 16 critical infrastructure sectors in discussion with Russian President Vladimir Putin reinforced the international expectations of "off-limits" targets. In addition, G7 leaders formally launched the Partnership for Global Infrastructure and Investment at the June 2022 summit, where President Biden announced a $200 billion investment to counter China's Belt and Road Initiative.[92] The establishment of the new Bureau of Cyberspace and Digital Policy further advances the implementation of this recommendation simply by increasing the personnel and resources available to participate in international cyber norms forums and other bilateral and multilateral discussions on expectations for responsible state behavior in cyberspace.

Pillar 3: Promote National Resilience

Promote National Resilience			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
3.1	Codify Sector-Specific Agencies as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk	Legislation Passed in FY21 NDAA; Funding Appropriated	
3.1.1	Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy	Legislation Proposed	
3.1.2	Establish a National Cybersecurity Assistance Fund	Legislation Proposed	
3.2	Develop and Maintain Continuity of the Economy Planning	Legislation Passed in FY21 NDAA; Further Appropriations Required	
3.3	Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"	Legislation Passed; Funding Appropriated	
3.3.1	Designate Responsibilities for Cybersecurity Services Under the Defense Production Act	Executive Action Taken	
3.3.2	Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts	Legislation Proposed	
3.3.3	Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts	Executive Action Underway; Further Action Required	
3.3.4	Expand Coordinated Cyber Exercises, Gaming, and Simulation	Appropriations in FY21 and FY22 Omnibus	
3.3.5	Establish a Biennial National Cyber Tabletop Exercise	Legislation Passed in FY21 NDAA	
3.3.6	Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard	Legislation Passed in FY21 NDAA; Required Report Pending	
3.4	Improve the Structure and Enhance Funding of the Election Assistance Commission	Legislation Passed in the House; Partial Funding Appropriated	
3.4.1	Modernize Campaign Regulations to Promote Cybersecurity	Legislation Proposed	
3.5	Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations	Legislation Needed; Further Appropriations Required	
3.5.1	Reform Online Political Advertising to Defend against Foreign Influence in Elections	Legislation Proposed	

Recommendation 3.1 – Codify Sector-Specific Agencies Into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk: This recommendation was implemented by FY21 NDAA Section 9002, which codified Sector Risk Management Agencies (SRMAs) into law. The legislation also requires a report on the methodology used to evaluate the incumbent system of sector-specific agencies and recommendations for revising the current list of critical infrastructure sectors. It also requires an ongoing process to review and revise the list of critical infrastructure sectors and subsectors.[93] The secretary of homeland security submitted the initial report to appropriate congressional committees in November 2021. The report provides a detailed description of the various systems and processes currently in place for protecting critical infrastructure, a history of how the U.S. government arrived at these systems, and a thoughtful assessment of their current performance. However, it does not provide clarity on how these systems are evaluated on an ongoing basis to ensure that they have a mechanism to adapt to a changing landscape of what is considered "critical," nor does it evaluate disparities in capability or effectiveness among SRMAs. In order for this recommendation to achieve long-term success, executive action will need to be taken to provide clarity and processes for ongoing evaluation of the designation of critical infrastructure sectors and the frameworks used to protect them. In addition, to ensure that all SRMAs are equipped to provide a consistent level of support to their respective sectors, Congress must ensure that appropriations are aligned with the mission assigned. The FY22 funding bill provided a monumental increase of $39 million for SRMA management above the FY22 request at CISA.[94] This appropriation will enable CISA to make dramatic improvements to its ability to support the critical infrastructure sectors that it serves, as well as support all SRMAs across the federal government. Outside of CISA, SRMA funding was distinctly more modest. Despite repeated recommendations from the CSC's congressional commissioners, the Department of Treasury has received no increase in funding dedicated to enhancing its role as the SRMA to the financial services sector. Similarly, the Environmental Protection Agency (EPA), the SRMA for water and wastewater infrastructure, would be far better positioned to address its critical role if it received increased funding, as highlighted in a November Foundation for Defense of Democracies report.[95]

Recommendation 3.1.1 – Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy: While the Senate's United States Innovation and Competition Act of 2021 had included the National Risk Management Act of 2021, introduced by Senator Hassan along with CSC Commissioner Senator Ben Sasse (R-NE),[96] the final version of the CHIPS and Science Act did not. The provision, however, is being introduced in the Senate for the FY23 NDAA. If it passes, it would direct the secretary of homeland security, acting through the CISA director, to "establish a recurring process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them."[97] This process is to be followed within a year by a national critical infrastructure resilience strategy "designed to address the risks identified by the Secretary" during the course of the national risk management cycle. This recommendation is not yet implemented and is awaiting legislative action.

Recommendation 3.1.2 – Establish a National Cybersecurity Assistance Fund: The Commission staff drafted and shared legislation to establish a National Cybersecurity Assistance Fund, which would support projects and programs that build resilience in public and private infrastructure. The proposal was worked with the relevant congressional committees but ultimately was not introduced during the 2021 legislative cycle. Congressional commissioners will continue to work on this provision as it is critical to ensuring that single point failures and other fragile areas in national critical infrastructure are identified and remediated prior to a significant cyber event. Funding in the Infrastructure Investment and Jobs Act for state and local cybersecurity grants, however, helps improve pre-incident resilience.[98]

Recommendation 3.2 – Develop and Maintain Continuity of the Economy (COTE) Planning: This recommendation was implemented by FY21 NDAA Section 9603, which authorized the development of a COTE plan. However, successfully carrying out such a plan will require a clear indication of which department or agency will lead it, and the effort will likely require additional funding. The FY22 appropriations report did provide an increase of $200,000 above the president's budget request for CISA to develop a COTE plan.[99] However, effective execution of Section 9603 will require a significantly greater scope of effort than the funding provided indicates. In particular, the legislation calls on CISA to create a plan every three years, requiring ongoing analysis of a diverse range of issues at a very granular level. Funding the personnel needed for this effort will be key to effective implementation. In the spring of 2022, the White House tasked CISA with leading the effort, some 15 months after the law was initially passed.

Recommendation 3.3 – Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund": Senators Gary Peters (D-MI) and Rob Portman (R-OH) first introduced the Cyber Response and Recovery Act of 2021,[100] bipartisan legislation with provisions that implemented this recommendation. The legislation boosts resources for the U.S. government in protecting the nation's critical infrastructure from significant cyber incidents. It was later passed into law in the Infrastructure Investment and

Jobs Act.[101] The legislation details a process by which the secretary of homeland security, in consultation with the NCD, can declare that a significant incident has occurred or will occur imminently. Upon declaration of a significant incident, the CISA director will coordinate response activities, which may involve public and private entities as well as state and local governments. The legislation also establishes a Cyber Response and Recovery Fund to support these efforts and appropriates $20 million for the fund in FY22 and each subsequent year through FY28.

Recommendation 3.3.1 – Designate Responsibilities for Cybersecurity Services Under the Defense Production Act: The Commission initially anticipated significant resistance to this recommendation. However shifting attitudes towards the use of the Defense Production Act in nontraditional areas during the Trump and Biden administrations and the increased urgency of cybersecurity issues led to a reevaluation of the need for legislation to implement this recommendation.[102] While cybersecurity industry leaders have expressed some concern as to how the use of Defense Production Act authorities might impact their operations and commitment to their other customers,[103] implementation of this recommendation no longer appears to face the substantial barriers the Commission anticipated.

Recommendation 3.3.2 – Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts: This recommendation is intended to clarify the circumstances under which entities responding at the direction of the federal government to a cybersecurity incident are insulated from liability for civil damages, fines, or penalties. Commission staff drafted legislation in support of this recommendation, but Congress has not introduced it. CSC 2.0 staff will continue to conduct research and analysis to meet the intent of this recommendation.

Recommendation 3.3.3 – Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts: While this recommendation has not been implemented as the Commission originally conceived, several activities are currently underway that align with the overall intent of the recommendation. In 2021, the Executive Order on Improving the Nation's Cybersecurity requires the development of incident response playbooks.[104] The FY22 NDAA requires updates and stakeholder outreach around the National Cyber Incident Response Plan.[105] Meanwhile, CISA established the Joint Cyber Defense Collaborative (JCDC) in August 2021,[106] which continues to expand its connections with the private sector to improve planning.[107] For example, CISA officials successfully handled the widespread exploitation of the Log4shell software vulnerability (Log4j) through the JCDC. JCDC members quickly convened to share information about the Log4j vulnerability, operationalizing public-private sector partnerships. Through the JCDC, CISA informed federal agencies to patch devices containing the Log4shell vulnerability, created a crowdsourced GitHub repository displaying vulnerable products and available patches, and provided resources to small- and medium-sized enterprises.[108]

Recommendation 3.3.4 – Expand Coordinated Cyber Exercises, Gaming, and Simulation: Section 1547 of the FY22 NDAA implemented this recommendation,[109] but the National Cyber Exercises Program requires further appropriations to cement implementation. The Consolidated Appropriations Act, 2021 provided nearly $22.8 million to the National Infrastructure Simulation Analysis Center.[110] Subsequently, the FY22 appropriations increased the budget for exercises within JCDC specifically by an additional $2,244,000.[111] Collectively, these appropriations are adequate for this recommendation's implementation; however, long-term success will still require action from the executive branch to ensure engagement with the wide community of relevant stakeholders.

Recommendation 3.3.5 – Establish a Biennial National Cyber Tabletop Exercise: The Commission considered this recommendation to be implemented in 2021 when Section 1744 of the FY21 NDAA requires the secretary of homeland security — in coordination with the director of national intelligence, the attorney general, and the secretary of defense — to conduct a minimum of four exercises before 2033. The three-day Cyber Storm VIII exercise took place in March 2022, involving more than 2,000 stakeholders.[112]

Recommendation 3.3.6 – Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard: This recommendation was implemented by FY21 NDAA Section 1729, which requires the secretary of defense to evaluate the rules and standards pertaining to the use of the National Guard in response to a cyber incident. The report on this evaluation has not yet been submitted to Congress. Once this report is reviewed, further action may still be needed to improve the National Guard's ability to respond in the event of a major cyber incident.

Recommendation 3.4 – Improve the Structure and Enhance Funding of the Election Assistance Commission: In 2020 and 2021, Congress and the executive branch took several major steps toward implementing this recommendation. The Consolidated Appropriations Act, 2021 provided an increase in funding of just under $2 million for the U.S. Election Assistance Commission (EAC).[113] CSC commissioners Representatives Jim Langevin (D-RI) and Gallagher also co-sponsored an amendment to H.R. 1 that

would clarify the duties of the EAC as they relate to cybersecurity and establish the position of the Senior Cyber Policy Advisor.[114] The House of Representatives passed H.R. 1, but the Senate did not take up the bill. In addition to this legislative activity, the EAC itself voted to approve an update to its Voluntary Voting System Guidelines.[115] The progress on implementation of this recommendation continued in 2021–2022, when the omnibus appropriations for FY22 increased the EAC's funding by $3 million, from $17 million to $20 million.[116] Notably, the report for the House version of the bill specifically called out cybersecurity, saying, "While Congress has made significant investments in election security, the funding has been inconsistent, unpredictable, and insufficient to meet the vast need across all the States and territories. Congress must provide a consistent, steady source of Federal funds to support State and local election officials on the frontlines of protecting U.S. elections."[117] While elements of this recommendation remain outstanding, particularly the permanent establishment of a Cyber Policy Advisor, this recommendation has been partially implemented. The president's budget has requested an increase for FY23 to $30,087,000, more than $10 million above current levels,[118] which would significantly advance the recommendation if funded. Additionally, the president's budget for FY23 proposes $10 billion in elections assistance funding to be allocated over ten years.[119]

Recommendation 3.4.1 – Modernize Campaign Regulations to Promote Cybersecurity: The Commission recommended amending the Federal Election Campaign Law to expressly permit corporations to provide cybersecurity assistance for free or at a reduced cost to political campaigns when such assistance is provided on a nonpartisan basis. While Congress has not introduced CSC staff-drafted legislation, CISA continues to provide election security resources,[120] with similar initiatives led by non-profit organizations in preparation for the midterm elections.[121] This differs from the Commission's recommendation because it is not legislative in nature, but these efforts broadly align with the intent of this recommendation.

Recommendation 3.5 – Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations: Prior to this year, CSC staff drafted legislation to establish an educational grant program and request a GAO report. In late 2021, the Commission added to these two lines of effort through its white paper on countering disinformation, which proposed a Civic Education Task Force[122] and several other measures to promote education as a tool for building resilience to disinformation. The CSC's congressional commissioners wrote a letter to the appropriations committees recommending additional funding for the Institute for Education Sciences and the National Defense Education Program, which was not included in the FY22 spending bill. The CSC's congressional commissioners are pursuing this issue again in FY23 appropriations.

Recommendation 3.5.1 – Reform Online Political Advertising to Defend Against Foreign Influence in Elections: CSC staff proposed legislation in support of this recommendation. That draft legislation would amend the Federal Election Campaign Act to implement restrictions on the purchase of advertising on the Internet akin to the limitations on foreign purchases of advertising in traditional media.[123] This proposal has not yet been introduced in Congress.

Pillar 4: Reshape the Cyber Ecosystem Toward Greater Security

Reshape the Cyber Ecosystem Toward Greater Security			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
4.1	Establish and Fund a National Cybersecurity Certification and Labeling Authority	Legislation Proposed; Related Executive Order Issued; Executive Action Required	
4.1.1	Create or Designate Critical Technology Security Centers	Legislation Proposed; Partial Funding Appropriated	
4.1.2	Expand and Support the National Institute of Standards and Technology Security Work	Legislation Passed; Funding Appropriated	
4.2	Establish Liability for Final Goods Assemblers	Faces Significant Barriers to Implementation	

Reshape the Cyber Ecosystem Toward Greater Security			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
4.2.1	Incentivize Timely Patch Implementation	Executive Action Required; Legislation Possible; Funding Required	
4.3	Establish a Bureau of Cyber Statistics	Legislation Proposed	
4.4	Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications	Partial Implementation via Legislation Passed in FY21 NDAA	
4.4.1	Establish a Public-Private Partnership on Modeling Cyber Risk	Executive Order Proposed	
4.4.2	Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events	Executive Order Proposed; Partial Implementation via Legislation Passed in FY21 NDAA	
4.4.3	Incentivize Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities	Implemented via Executive Order; Legislation Proposed	
4.4.4	Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements	Legislation Proposed; Executive Action Proposed	
4.5	Develop a Cloud Security Certification	Legislation Proposed; Executive Order Issued; Appropriations Required	
4.5.1	Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments	Legislation Required; Additional Authorization/ Appropriations Required	
4.5.2	Develop a Strategy to Secure Foundational Internet Protocols and Email	Partial Implementation via Legislation Passed in FY21 and FY22 NDAA; Further Implementation Possible via Executive Action or Legislation	
4.5.3	Strengthen the U.S. Government's Ability to Take Down Botnets	Executive Action Taken; Legislation Introduced	
4.6	Develop and Implement an ICT Industrial Base Strategy	In Process via Executive Order	
4.6.1	Increase Support to Supply Chain Risk Management Efforts	Full Implementation via Executive Order and CHIPS and Science Act	
4.6.2	Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies	Legislation Passed; Funding Appropriated	
4.6.3	Strengthen the Capacity of the Committee on Foreign Investment in the United States	Executive Action Taken; Partial Funding Appropriated	
4.6.4	Invest in the National Cyber Moonshot Initiative	Legislation Passed; Partial Funding Appropriated	
4.7	Pass a National Data Security and Privacy Protection Law	Legislation Proposed	
4.7.1	Pass a National Breach Notification Law	Related Legislation Proposed	

Recommendation 4.1 – Establish and Fund a National Cybersecurity Certification and Labeling Authority: In 2021, Senators King and Sasse introduced the Defense of United States Infrastructure Act of 2021, which included provisions that would establish a National Cybersecurity Certification and Labeling Authority (NCCLA).[124] Commission staff also drafted a variant of this legislation calling for a report to Congress on what such an authority might look like in implementation. While many provisions from the Defense of United States Infrastructure Act were considered for inclusion in an amendment to the Senate version of the FY22 NDAA, this provision ultimately was not. The CSC's congressional commissioners are working this year to reengage on this legislation. Meanwhile, the 2021 Executive Order on Improving the Nation's Cybersecurity began to lay the groundwork for future certification and labeling efforts[125] on which the administration can build on in the coming year. In particular, NIST issued criteria for Internet of Things (IoT) device and software security, indicating the desired outcomes of secure products.[126] However, further executive action (which may be expedited with a congressional mandate) will be needed to map these criteria to more concrete standards that can serve as the basis for a labeling system.

Recommendation 4.1.1 – Create or Designate Critical Technology Security Centers: Legislation that would implement this recommendation was included in the FY22 and FY23 House versions of the NDAA,[127] and Senators King and Sasse introduced a parallel provision in the Defense of United States Infrastructure Act.[128] However, the provision was not included in the final FY22 NDAA, and the FY23 NDAA is still pending. While full implementation of this recommendation is not possible without further authorizing legislation, the appropriations provisions of the Infrastructure Investment and Jobs Act does designate $157,500,000 for the Science and Technology Directorate of the Department of Homeland Security (DHS). The appropriation is to be used for, among other things, "research supporting security testing capabilities relating to telecommunications equipment, industrial control systems, and open source software."[129] As a result, this recommendation is considered partially implemented.

Recommendation 4.1.2 – Expand and Support the National Institute of Standards and Technology Security Work: Implementation of this recommendation is principally contingent on an increase in funding to the National Institute of Standards and Technology in support of the cybersecurity and privacy budget. While the president's budget request for FY22 increased funding to NIST organization-wide by nearly 45 percent relative to the FY21 budget, the cybersecurity and privacy budget increased by only six percent.[130] This growth is out of step with the expansion of responsibilities assigned to NIST in the Executive Order on Improving the Nation's Cybersecurity,[131] as well as an expanded workforce development role mandated in FY21 NDAA Section 9401. The Consolidated Appropriations Act, 2022 increased appropriations for cybersecurity and privacy at NIST by $1.5 million,[132] which falls drastically short of the $54 million increase over the FY22 request that the CSC's congressional commissioners recommended in a letter to congressional appropriators for FY23. The passage of the CHIPS and Science Act provides clarity on NIST's authority for cybersecurity and privacy activities. Section 10223 of the act allows NIST to provide consensus-based technical standards and guidance on technologies that enhance software and cloud security and privacy.[133]

Recommendation 4.2 – Establish Liability for Final Goods Assemblers: As was the case in the prior year, this recommendation has encountered significant barriers to implementation. Should future events generate the impetus needed to implement the proposal, Commission staff has drafted sample legislation.[134]

Recommendation 4.2.1 – Incentivize Timely Patch Implementation: Ultimately, implementation of this recommendation will require executive action to update existing guidance. Congressional appropriators considered positive steps by including report language in both the House and Senate versions of the FY22 appropriations bill that requires NIST to revise and update SP 800-40, the Guide to Enterprise Patch Management Technologies.[135] However, Congress dropped the suggested language in the final report.

Recommendation 4.3 – Establish a Bureau of Cyber Statistics: Implementation of this recommendation requires authorizing language, and Commission staff and the CSC's congressional commissioners worked in support of this recommendation through the 2021 legislative cycle. The provision was introduced as a part of the Defense of United States Infrastructure Act.[136] Ultimately, however, the provision was not included in the FY22 NDAA, which could have served as a vehicle to expedite the passage of the legislation. Representative Jim Langevin (D-RI) continued the Commission's efforts by introducing the recommendation as an amendment to the FY23 NDAA, but it was not included.[137]

Recommendation 4.4 – Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications: Full implementation of this recommendation will require executive action to direct a federally funded research and development center to develop a training and certification program for insurance professionals. Section 9005 of the FY21 NDAA mandated a GAO study on the cybersecurity insurance market, which partially serves to implement this recommendation.[138] Subsequently, the GAO published a report to congressional committees, noting growing risks pose uncertainty in the evolving cybersecurity insurance market.[139]

On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) issued proposed amendments to its rules on cybersecurity, risk management, strategy, governance, and incident disclosure by public companies... If these proposed rules become permanent, this will accomplish the intent of the CSC recommendation.

Recommendation 4.4.1 – Establish a Public-Private Partnership on Modeling Cyber Risk: This recommendation will require executive action for full implementation, but progress could be spurred through appropriations report language. The CSC's congressional commissioners recommended language for the FY23 appropriations bill in support of a working group that would develop models and frameworks to help price cyber risk and identify ways to inform more accurate risk models. This language was not included in the final bill but will remain a recommendation in the coming year.

Recommendation 4.4.2 – Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events: While this recommendation was partially implemented through FY21 NDAA Section 9005, further action is needed to fully implement the recommendation.[140] For instance, the May 2021 GAO report on cyber insurance examined what types of cyber incidents fall under the Treasury Department's definition of "certified acts of terrorism."[141] Subsequently, the GAO published a report in June 2022 providing recommendations for executive action to assess which risks and catastrophic cyber incidents affecting the critical infrastructure require a federal insurance response.[142] Thus, establishing consistent standard definitions of cyber incidents and analyzing key trends in cyber insurance is necessary to address the cyber insurance industry. New legislation or an amendment to the Terrorism Risk Insurance Act could be needed.

Recommendation 4.4.3 – Incentivize Information Technology Security Through Federal Acquisition Regulations and Federal Information Security Management Act Authorities: This recommendation was considered implemented in 2021 through Executive Order 14028, titled "Improving the Nation's Cybersecurity." Notably, however, a legislative push for the Federal Information Security Modernization Act of 2021,[143] introduced by Senators Peters and Portman through the Senate Homeland Security and Government Affairs Committee, would have had a significant impact on incentivizing information security. A companion version of the bill, the Federal Information Security Modernization Act of 2022, was introduced in the House in January.[144] While this legislative proposal was developed outside the Commission, its passage would achieve the intent of this recommendation.

Recommendation 4.4.4 – Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements: Implementation of this recommendation may require legislation amending the Sarbanes-Oxley Act to clarify reporting requirements and cybersecurity oversight in publicly traded companies. On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) issued proposed amendments to its rules on cybersecurity, risk management, strategy, governance, and incident disclosure by public companies subject to the requirements of the Securities Exchange Act of 1934.[145] The SEC set April 2023 as the target date to take final action.[146] If these proposed rules become permanent, this will accomplish the intent of the CSC recommendation.

Recommendation 4.5 – Develop a Cloud Security Certification: As envisioned by the Commission, the National Cybersecurity Certification and Labeling Authority (Recommendation 4.1) would partner with NIST, the Office of Management and Budget, and DHS to develop a certification to attest to the security of cloud services. The recommendation also outlined a process for developing cloud security metrics and standards and called for an update to the Federal Risk and Authorization Management Program (FedRAMP). While the establishment of the NCCLA would greatly expedite the implementation of this recommendation as a whole, policymakers can still pursue major elements of the recommendation absent the creation of the NCCLA. Meanwhile, the House and Senate versions of the FY22 omnibus appropriation urged the executive to develop guidelines for secure cloud adoption, but it did not make the final version.[147] The May 2021 Executive order on Improving the Nation's Cybersecurity called for improved agency plans to secure cloud services and updates to FedRAMP.[148] Notably, the successful execution of these changes will require funding for expanded lines of work, particularly at NIST. As is also the case for Recommendation 4.1.2 above, the history of limited growth in appropriations for NIST's cybersecurity and privacy budget function is concerning. The CSC's congressional commissioners have written letters to congressional appropriators urging increased resources for this important funding priority.

Recommendation 4.5.1 – Incentivize the Uptake of Secure Cloud Services for Small- and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments: The State and Local Cybersecurity Improvement Act — passed into law in the Infrastructure Investment and Jobs Act — provides grant funding that can be used to implement, develop, or revise cybersecurity plans or assist with activities to address imminent cybersecurity threats.[149] While the $1 billion appropriated over five years for this grant program is not exclusively intended for incentivizing migration to more secure cloud services, it can certainly be used to implement this recommendation. Accordingly, this recommendation is considered partially implemented, noting that states and localities must still choose to use the funding for that purpose. However, small- and medium-sized businesses are not included in this program.

Recommendation 4.5.2 – Develop a Strategy to Secure Foundational Internet Protocols and Email: This recommendation specifically addresses securing three elements: Border Gateway Protocol (BGP), the Domain Name System (DNS), and email communication via the Domain-based Message Authentication, Reporting, and Conformance (DMARC) standard. Section 9006 of the FY21 NDAA called for the creation of a strategy to implement DMARC, thus partially implementing this recommendation last year.[150] In FY22, the Commission again pursued legislation to secure BGP and DNS, but the FY22 NDAA only covered the security of DNS in Section 1524. Additional action is necessary to address the security of BGP.

Recommendation 4.5.3 – Strengthen the U.S. Government's Ability to Take Down Botnets: In June 2021, a bipartisan group of senators reintroduced the proposed International Cybercrime Prevention Act of 2021.[151] Section 4 of that legislation would implement the Commission's recommendation to ensure law enforcement has the statutory authority to respond to botnets engaged in non-fraudulent but still abusive behaviors, such as DDoS attacks or email harvesting. Enabling the U.S. government to work with private industry and international partners to take down botnets could have a global impact. For example, in April 2022, the Department of Justice announced a court-authorized takedown of a botnet associated with the Russian military intelligence directorate's Sandworm hacking group. Working with law enforcement agencies in the United States and United Kingdom and a Seattle-based network security vendor called WatchGuard, the operation successfully removed Cyclops Blink, a malware used to infect thousands of devices for the botnet's command and control (C2), severing the infected devices from Sandworm's C2. [152] Attorney General Merrick Garland confirmed that the operation disabled Russia's control over these infected devices "before the botnet could be weaponized."[153] The legislation has not yet passed the Senate and has not been introduced in the House.

Recommendation 4.6 – Develop and Implement an Information and Communications Technology Industrial Base Strategy: This recommendation, which forms the core of the Commission's white paper on "Building a Trusted ICT Supply Chain," is in progress as a function of the February 2021 Executive Order on America's Supply Chains.[154] This order requires the assessment of key elements of the supply chain, including semiconductor manufacturing and the ICT industrial base. These reports will then be used to inform recommendations to the president on strengthening these supply chains and establishing a quadrennial supply chain review. As a result, this recommendation is nearing implementation, but these reports and presidentially mandated recommendations do not constitute an industrial base strategy as such. Therefore, full implementation requires further executive action.

Recommendation 4.6.1 – Increase Support to Supply Chain Risk Management Efforts: As with Recommendation 4.6, the February 2021 executive order set the implementation of this recommendation in motion with a series of required reports.[155] However, this recommendation further calls for mechanisms to share information on supply chain threats with the private sector, thus improving the private sector's ability to manage its own risk of vulnerabilities introduced through the supply chain. Similar to the previous year, the FY22 NDAA continues to emphasize the importance of supply chain readiness and domestic supply chain preference. For example, Section 847 calls for a joint effort between the State Department and the Department of Defense (DoD) to develop and implement a plan to reduce the nation's reliance on "sources for services, supplies, or materials" from countries like North Korea, China, Russia, and Iran to mitigate the risks to the defense supply chain.[156] Other provisions included in the FY22 NDAA continue the efforts from the previous year, but legislative action is required to address supply chain risks as a national security concern and for full implementation of this recommendation. The passage of the CHIPS and Science Act provides further guidance on software supply chain security practices. Section 10224 calls for public-private collaboration to produce guidance and best practices "to identify, assess, and manage cybersecurity risks over the full lifecycle of software products."[157] Furthermore, Section 10253 establishes a voluntary National Supply Chain Database that would assess U.S. manufacturers' capabilities to minimize supply chain disruptions.[158] With the passage of the CHIPS and Science Act, this recommendation is considered fully implemented.

Recommendation 4.6.2 – Commit Significant and Consistent Funding Toward Research and Development in Emerging Technologies: A number of measures have benefited this recommendation in the past year, and the Consolidated Appropriations Act, 2022 designated tens of millions of dollars for artificial intelligence and machine learning (in both basic research and advanced technologies), high-performance computing, quantum computing, and other areas.[159] The passage of the CHIPS and Science Act implements this recommendation. Section 10381 creates a new Directorate for Technology and Innovation at the National Science Foundation,[160] and Section 10389 authorizes $6.5 billion in appropriations over five years for the Directorate to carry out "research, development, and commercialization of innovation" in multidisciplinary technology focus areas.[161] Successful execution of this recommendation requires further appropriations, particularly expenditure on priorities like supporting multi-sector partnerships; building a highly-skilled, diverse workforce; and supporting research environments that align with American values. Evaluating the success of this implementation will be a very long-term endeavor. Congressional appropriators should ensure the consistency of the funding for this recommendation when implemented in parallel with legislative action needed to implement this recommendation.

Recommendation 4.6.3 – Strengthen the Capacity of the Committee on Foreign Investment in the United States: The House and Senate versions of the FY22 appropriations bill raised this issue specifically, encouraging "the Federal Judicial Center, through Education and Training program, to support the education of bankruptcy judges on how bankruptcy court decisions may impact national security."[162] But this provision did not make it into the final bill. However, the FY23 president's budget includes a 25 percent increase in funding for the Committee on Foreign Investment in the United States,[163] in addition to the House FY22 appropriations for bankruptcy judges,[164] partially implementing this recommendation.

Recommendation 4.6.4 – Invest in the National Cyber Moonshot Initiative: The Initiative was created in 2018 to "make the Internet safe and secure for the functioning of Government and critical services for the American people by 2028."[165] The FY21 NDAA addressed a number of the principles laid out by the Cyber Moonshot Initiative, particularly the education pillar of the Initiative's work. The CHIPS and Science Act of 2022 similarly addressed numerous issues from the education, ecosystem, technology, and policy pillars of the Cyber Moonshot Initiative.[166] While the progress of the past two years has been positive, further investment in the Initiative's work is critical.

Recommendation 4.7 – Pass a National Data Security and Privacy Protection Law: As was the case in the prior year, the Commission has encountered significant barriers to the implementation of this recommendation. However, as the costs to individuals of poor privacy protections continue to stack up, attitudes towards data security and privacy protection seem to be changing among lawmakers. The Commission has drafted and published legislation, making it available should there be an increased appetite to pursue the issue in the future.[167] The passage of the CHIPS and Science Act shows progress in establishing a standardized requirement for the collection, retention, and sharing of user data. Section 10375 establishes a National Secure Data Service demonstration project to test models for government-wide data linkage and access infrastructure. Under the National Science Foundation, the project aims to improve coordination across national data collection, including privacy and confidentiality protections, emphasizing the need to handle raw data and sensitive inputs securely.[168] Furthermore, there is proposed legislation on this issue. In June 2022, the House Energy and Commerce Committee introduced the American Data Privacy and Protection Act, which would create a federal consumer privacy law standardizing consumers' expectations on managing personal data and regulations for companies on how they could use that data.[169] The CSC 2.0 project will remain focused on this issue.

As the costs to individuals of poor privacy protections continue to stack up, attitudes towards data security and privacy protection seem to be changing among lawmakers. ... The passage of the CHIPS and Science Act shows progress in establishing a standardized requirement for the collection, retention, and sharing of user data.

Recommendation 4.7.1 – Pass a National Breach Notification Law: Alongside Recommendation 5.2.2, which pertains to a mandatory incident reporting law, the Commission anticipated significant reservations about the implementation of this recommendation. However, the increasing prevalence of — and congressional focus on[170] — major cybersecurity incidents throughout 2020-2021 led to shifting attitudes, making this proposal more feasible. The Cyber Incident Reporting for Critical Infrastructure Act of 2021 requires CISA to provide a framework for covered entities when reporting cyber incidents and ransomware payments to CISA.[171] While that law could be used as a model for voluntary sharing of information about cyber incidents, further legislative action is required for a national breach notification law.

Pillar 5: Operationalize Cybersecurity Collaboration With the Private Sector

Operationalize Cybersecurity Collaboration With the Private Sector			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
5.1	Codify the Concept of "Systemically Important Critical Infrastructure"	Legislation Proposed	
5.1.1	Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector	Legislation Proposed	
5.1.2	Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities	Legislation Proposed	
5.1.3	Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities	Legislation Passed in FY21 NDAA	
5.2	Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information	Legislation Proposed	
5.2.1	Expand and Standardize Voluntary Threat Detection Programs	Legislation Passed; Funding Appropriated	
5.2.2	Pass a National Cyber Incident Reporting Law	Full Implementation via the Cyber Incident Reporting for Critical Infrastructure Act of 2022	
5.2.3	Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors	Legislation Proposed	
5.3	Strengthen an Integrated Cyber Center Within CISA and Promote the Integration of Federal Cyber Centers	Legislation Passed in FY21 NDAA; Legislation and Appropriations May Be Required for FY23; Required Report Pending	
5.4	Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency	Legislation Passed in FY21 NDAA; Funding Appropriated for FY21 and FY22	
5.4.1	Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives	Legislation Passed in FY21 and FY22 NDAAs	
5.4.2	Expand Cyber Defense Collaboration With ICT Enablers	Legislation Passed in FY22 NDAA	

Recommendation 5.1 – Codify the Concept of "Systemically Important Critical Infrastructure": Commissioners, staff, and partners on the Hill engaged at length to advocate for this proposal's inclusion in the FY22 NDAA, including gathering extensive input from government stakeholders and industry groups and proposing an alternative implementation plan for the proposal. Over the course of the drafting process, Commission and legislative staff worked on adding greater detail, particularly to elements of the bill that dealt with the added benefits and burdens that Systemically Important Critical Infrastructure entities would receive. In particular, sections specifying intelligence support to the private sector and regulatory requirements matured significantly through revisions. The proposal was introduced in the Defense of United States Infrastructure Bill,[172] but ultimately was not included in the FY22 NDAA. Commissioners remain convinced that the government and private sector must work together to explicitly identify the most important assets within our national critical infrastructure to ensure that additional

efforts are made to both protect these assets before an incident and rapidly recover these assets after an incident. Appropriate language is currently included in the House version of the FY23 NDAA, and this remains a top priority for the congressional commissioners and other lawmakers.

Recommendation 5.1.1 – Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector: A pivotal element of many CSC recommendations is increased and improved information sharing with the private sector. Putting this into action most effectively requires an improved understanding of the resources, procedures, policies, and authorities available to the intelligence community to support the private sector. Commission staff has drafted a proposal directing the executive branch to carry out a review,[173] and CSC 2.0 will remain focused on this issue.

Recommendation 5.1.2 – Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities: While the FY22 NDAA made strides in intelligence support and coordination with the private sector, those efforts focused on DoD and DHS via CISA, rather than the Office of the Director of National Intelligence. Making this recommendation further unique, it calls for a recurrent process by which critical infrastructure sectors' input can inform national intelligence priorities. Critical infrastructure owners and operators can provide critical insight into known gaps in their own cybersecurity or nodes in their operations that may be particularly critical, which can help identify areas that may be targeted by future nation-state adversaries. The provision of this information can also serve as a feedback mechanism to help focus intelligence collection on areas where critical infrastructure owners and operators have identified vulnerabilities or are limited in their own information-gathering efforts. The Commission staff has drafted a legislative proposal for this recommendation,[174] but the changes could also be carried out via executive branch action in the absence of specific authorizing legislation.

Recommendation 5.1.3 – Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities: This recommendation has been implemented. Section 1716 of the FY21 NDAA provided administrative subpoena authority to CISA.[175] That authority allows the agency to identify and contact the owner or operator of a device related to critical infrastructure in the event of a security vulnerability, contingent on certain limitations on the information to be obtained, coordination with other federal agencies, notification processes, and other procedures.

Recommendation 5.2 – Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information: The House of Representatives included a provision in its version of the FY22 NDAA that would have implemented this recommendation by establishing a Cyber Threat Information Collaboration Environment.[176] However, it was not included in the final version of the FY22 NDAA, despite a parallel provision in Senators King and Sasse's Defense of United States Infrastructure Act.[177] As was the case with many of the legislative provisions with a legacy in the CSC's recommendations, this proposal requires jurisdictional relief from many congressional committees. Because the chair and ranking member of each committee of jurisdiction must agree to grant jurisdictional relief for the proposal to be included in the NDAA, these cross-jurisdictional proposals are especially challenging. Overcoming these challenges and supporting the proposal is a key priority for the congressional commissioners. The House version of the FY23 NDAA again includes this provision. The issuance of the May 2021 Executive Order on Improving the Nation's Cybersecurity may also help build a path for this recommendation by calling for improvements to information sharing between federal departments and agencies.[178]

Recommendation 5.2.1 – Expand and Standardize Voluntary Threat Detection Programs: FY22 NDAA Section 1548 codified CyberSentry, a voluntary program through CISA that provides continuous monitoring and detection of cybersecurity threats on critical infrastructure owners' and operators' networks. Additionally, the Consolidated Appropriations Act, 2022 provided a remarkable $95,549,000 above the president's budget request to support CyberSentry and other voluntary threat detection programs that place sensors where the operational technology and information technology components of critical infrastructure networks meet. Appropriators specified that most of the funding will be used towards deploying sensors and developing tools to analyze incoming data; however, more than $13 million of the funds may also be used for operations and program management.[179] In light of both authorization and appropriation, this recommendation is considered implemented, but long-term success is still a function of the execution of these programs.

Recommendation 5.2.2 – Pass a National Cyber Incident Reporting Law: After years of efforts to incentivize and promote voluntary reporting among private sector victims of cyberattacks, the past year saw significant shifts in attitudes toward mandatory incident reporting legislation.[180] The May 2021 Executive Order on Improving the Nation's Cybersecurity established an incident reporting requirement for federal contractors. The order also established a Cyber Safety Review Board, which

will improve access to information on incidents.[181] These measures represent meaningful progress, but the recommendation was finally fully implemented by Congress with the passage in March 2022 of the Cyber Incident Reporting For Critical Infrastructure Act of 2022 as Division Y of the Consolidated Appropriations Act, 2022.[182] The law will require certain private sector critical infrastructure companies to report to authorities if they have been the victim of a significant cybersecurity incident. Accordingly, this recommendation is considered fully implemented.

As one of the major achievements of the Commission's first year, the Joint Cyber Planning Office was implemented in Section 1715 of the FY21 NDAA. ... In FY22, Congress appropriated more than $16 million above the president's budget request... This funding puts the office — which CISA has rebranded as the Joint Cyber Defense Collaborative — off to a strong start.

Recommendation 5.2.3 – Amend the Pen Register Trap and Trace Devices Statute to Enable Better Identification of Malicious Actors: Commission staff proposed an amendment to the Pen Register Trap and Trace Devices Statute (18 U.S.C. §3121) that would increase the private sector's options to identify malicious actors and defend their networks. The proposal was not taken up by the chambers of Congress with which it was shared in the 2021 legislative year, but the congressional commissioners will continue to prioritize it.

Recommendation 5.3 – Strengthen an Integrated Cyber Center Within CISA and Promote the Integration of Federal Cyber Centers: FY21 NDAA Section 1731 implemented this recommendation by calling for a report on "Federal cybersecurity centers and the potential for better coordination of Federal cybersecurity efforts at an integrated cybersecurity center."[183] The report has not yet been submitted to Congress. Long-term success of this recommendation will depend on whether the findings of the report lead to better coordinated action, increased common situational awareness, production and utility of joint analysis, and overall better integration of planning efforts. As it matures, the newly formed Joint Cyber Defense Collaborative may serve many of these functions. Relatedly, long-term success will also depend on resources being made available to CISA for this purpose. The FY22 appropriations act's historic investment in CISA will be instrumental in ensuring this success, and appropriators should keep the importance of this investment in mind in future years.

Recommendation 5.4 – Establish a Joint Cyber Planning Cell Under the Cybersecurity and Infrastructure Security Agency: As one of the major achievements of the Commission's first year, the Joint Cyber Planning Office was implemented in Section 1715 of the FY21 NDAA. Congress appropriated $10,568,000 for the effort in FY21.[184] In FY22, Congress appropriated more than $16 million above the president's budget request,[185] which was itself an increase of $10 million over the FY21 appropriation.[186] This funding puts the office — which CISA has rebranded as the Joint Cyber Defense Collaborative — off to a strong start. The JCDC is now tasked with leading "the development of the Nation's cyber defense plans by working across the public and private sectors to unify deliberate and crisis action planning, while coordinating the integrated execution of these plans."[187] The president's budget for fiscal year 2023 includes a $14.7 million increase to continue the work of the JCDC.[188]

Recommendation 5.4.1 – Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives: This recommendation was partially implemented with the FY21 NDAA and then fully implemented with the passage of the FY22 NDAA. Section 1728 of the FY21 bill requires a review from DoD of current public-private cybersecurity initiatives but did not specify coordination with DHS and did not prescribe action beyond the review.[189] The FY22 bill bridged this gap with two provisions. Section 1512 authorizes DoD to provide cybersecurity support to critical infrastructure owners and operators, and Section 1513 requires a report outlining how DoD can provide support and assistance to CISA to increase awareness of cyber risks that affect information communication technology networks that support critical infrastructure.[190]

Recommendation 5.4.2 – Expand Cyber Defense Collaboration With ICT Enablers: Sections 1508 and 1550 of the FY22 NDAA implement this recommendation. Section 1508 requires U.S. Cyber Command to establish a voluntary process for engaging with information technology and cybersecurity companies.[191] Section 1550 establishes a pilot program at CISA to assess the feasibility of building voluntary partnerships with internet ecosystem companies, which are defined as those that provide "cybersecurity services, internet service, content delivery, Domain Name Service, cloud services, mobile telecommunications services, email and messaging services, internet browser services,"[192] and possibly others. The CISA director's task will then be to determine whether such partnerships could be used to find and stop malicious cyber actors using platforms owned by the companies.

Pillar 6: Preserve and Employ the Military Instrument of Power

Preserve and Employ Military Instruments of Power			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
6.1	Direct the DoD to Conduct a Force Structure Assessment of the Cyber Mission Force	Legislation Passed in FY21 NDAA	
6.1.1	Direct DoD to Create a Major Force Program Funding Category for U.S. Cyber Command	Legislation Passed in FY21 and FY22 NDAAs	
6.1.2	Expand Current Malware Inoculation Initiatives	Executive Action Taken; Further Action Required	
6.1.3	Review Delegation of Authorities for Cyber Operations	Legislation Passed in FY21 NDAA	
6.1.4	Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces	Executive Action Required	
6.1.5	Cooperate With Allies and Partners to Defend Forward	Executive Action Taken	
6.1.6	Require the DoD to Define Reporting Metrics	Legislation Required	
6.1.7	Assess the Establishment of a Military Cyber Reserve	Legislation Passed in FY21 NDAA; Required Report Pending	
6.1.8	Establish Title 10 Professors in Cyber Security and Information Operations	Related Legislation Passed in FY22 NDAA; Further Action Required	
6.2	Conduct Cybersecurity Vulnerability Assessment of Across the Nuclear Command, Control, and Communications and National Leadership Command Capability Systems & Continually Assess Weapon Systems' Cyber Vulnerabilities	Legislation Passed in FY21 and FY22 NDAAs; Related Executive Order Issued	
6.2.1	Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program	Partial Implementation via Legislation Passed in FY21 NDAA; Further Legislation Possible	
6.2.2	Require Threat Hunting on Defense Industrial Base Networks	Partial Implementation via Legislation Passed in FY21 NDAA; Further Legislation Possible	
6.2.3	Designate a Threat-Hunting Capability Across the Department of Defense Information Network	Legislation Passed in FY22 NDAA	
6.2.4	Assess and Address the Risk to National Security Systems Posed by Quantum Computing	Legislation Passed in FY21 NDAA	

Recommendation 6.1 – Direct DoD to Conduct a Force Structure Assessment of the Cyber Mission Force: Section 1706 of the FY21 NDAA mandated a force structure assessment that meets the intent of this recommendation. In testimony before the House Armed Services Committee in 2022, General Paul Nakasone, head of U.S. Cyber Command and the National Security Agency, reported that work on this assessment is underway.[193] The initial results of this assessment can be seen in Defense Department's requests to increase the National Mission Force by 14 Cyber Mission Teams (or 10 percent) from 2021 to 2024. This can be seen as a down payment on the requirements that will likely be identified in the force structure assessment.[194]

Recommendation 6.1.1 – Direct DoD to Create a Major Force Program Funding Category for U.S. Cyber Command: This recommendation, which was partially implemented by the FY21 NDAA, was fully implemented by Section 1507 of the FY22 NDAA. The earlier legislation — respectively in Sections 1711 and 1746 of the FY21 NDAA — removed a $75 million cap on spending and granted the Commander of U.S. Cyber Command some budget and acquisition authorities in excess of funding limits. Section 1507 of the FY22 NDAA further advances this progress by delegating the development of Cyber Command's budget request and justification to the Commander (exclusive of military pay and facility support).[195]

Recommendation 6.1.2 – Expand Current Malware Inoculation Initiatives: This recommendation advocates the expansion of programs through which the federal government supports private-sector defensive efforts by releasing to the public information — such as malicious code samples — that government actors have encountered during threat hunting or other activities. These efforts are ongoing, as exemplified in the 2021 release of malware samples connected to the SolarWinds compromise.[196] However, further opportunities to expand and refine the program exist by improving the granularity, timing, and actionability of information released by working with partners across government, in the private sector, and internationally. Further implementation of this recommendation can benefit from the new coordination mechanisms proposed in CSC recommendations.

Recommendation 6.1.3 – Review the Delegation of Authorities for Cyber Operations: This recommendation was implemented in FY21 NDAA Section 1706. The legislation calls for an "assessment of the need for further delegation of cyber-related authorities, including those germane to information warfare, to the Commander of United States Cyber Command."[197]

Recommendation 6.1.4 – Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces: The Standing Rules of Engagement and Standing Rules for the Use of Force for U.S. forces are more than 10 years old, despite a context that has changed dramatically over the intervening period. Implementation of this recommendation would require executive action to update these rules, ideally as part of the next Cyber Posture Review.

Recommendation 6.1.5 – Cooperate With Allies and Partners to Defend Forward: Implementation of this recommendation is based on executive action. In particular, the U.S. government could begin implementing this recommendation by reviewing the ways in which defend forward activities and persistent engagement may impact allies and partners and by assessing opportunities to expand collaboration. However, if these reviews are completed but not made publicly available, they would be difficult to use as a barometer of progress. With this in mind, externally visible actions show significant progress in this area. For example, the G7 leaders formally launched the Partnership for Global Infrastructure and Investment[198] at the June 2022 summit, upholding their commitment "to the framework of responsible state behaviour in cyberspace."[199] In addition, NATO released its 2022 Strategic Concept during its June summit, reaffirming last year's strategy that a cyberattack against one of its member states could potentially trigger Article 5 of the North Atlantic Treaty, meaning that a cyberattack against one of its member states could be considered an attack against the alliance as a whole.[200] There has been ongoing cooperation with allies and partners for persistent engagement. In the four years prior to May 2022, U.S. Cyber Command conducted 28 hunt-forward operations, deploying the Cyber National Mission Force to 16 nations.[201] General Nakasone stated these hunt forward operations were "directly in support of mission partners," bolstering the resilience of NATO allies and partners.[202]

Recommendation 6.1.6 – Require DoD to Define Reporting Metrics: The FY20 NDAA Section 1634 requires DoD to establish metrics to inform quarterly readiness assessments of the Cyber Mission Force.[203] The Commission's recommendation calls for the development of some metrics beyond just measures of readiness, such as metrics encompassing outcomes of defend forward activities at a range of levels. This change could be mandated legislatively but could also be carried out under existing authorization. Whether implemented through executive action or legislation, implementation of this recommendation will require clear metrics by which defend forward outcomes may be evaluated.

Recommendation 6.1.7 – Assess the Establishment of a Military Cyber Reserve: This recommendation was implemented through Section 1730 of the FY21 NDAA. The legislation requires DoD to carry out an "evaluation of reserve models tailored to the support of cyberspace operations for the Department."[204] This evaluation should include a discussion of alternative models for a

reserve force dedicated to cyber issues. This evaluation was due 270 days following the enactment of the FY21 NDAA but has not yet been submitted. Notably, while the Commission's recommendation focused on a uniformed cyber reserve, legislators have introduced proposals for a civilian cyber reserve as well.[205]

Recommendation 6.1.8 – Establish Title 10 Professors in Cyber Security and Information Operations: This recommendation could be implemented by the executive branch under the existing authorization; however, it could also be carried out through legislation and would likely have greater longevity if so implemented. The Commission staff drafted and shared with congressional committees a legislative proposal requiring a revision to the Joint Professional Military Education standards that would implement this recommendation. To date, this has not been implemented, but related legislation was included in the FY22 NDAA, which requires a talent management strategy.[206] That provision does not fully implement this recommendation, but it can serve as a starting point toward a more comprehensive approach to cyber education.

Recommendation 6.2 – Conduct a Cybersecurity Vulnerability Assessment Across the Nuclear Command, Control, and Communications and National Leadership Command Capability Systems & Continually Assess Weapon Systems' Cyber Vulnerabilities: Multiple pieces of legislation that meet the intent of this recommendation have passed into law in recent years. In the FY21 NDAA, Section 1712 requires periodic reviews of the vulnerabilities of major weapons systems and the critical infrastructure that those systems may require. Section 1747 of the FY21 NDAA requires DoD to establish a concept for operations needed to defend nuclear command and control from cyberattacks. Subsequently, in the FY22 NDAA, Section 1525 requires DoD to issue regular reports on the progress of the Strategic Cybersecurity Program, an effort that evaluates the cybersecurity of offensive cyber systems, long-range strike systems, nuclear deterrent systems, national security systems, and DoD critical infrastructure.[207] Section 1534 puts a deadline on an existing mandate for assessments of the cyber resilience of nuclear command and control systems. Finally, Section 1644 calls for an "independent review of the safety, security, and reliability of covered nuclear systems," which includes, but is not limited to, cybersecurity.[208] In addition to these legislative steps, the May 2021 Executive Order on Improving the Nation's Cybersecurity requires the secretary of defense to provide further details on cybersecurity practices for national security systems.[209] On January 19, 2022, President Biden signed a national security memorandum requiring DoD, the intelligence community, and other national security systems to employ the same network cybersecurity measures as federal civilian networks, as outlined in Executive Order 14028.[210]

Recommendation 6.2.1 – Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program: Section 1737 of the FY21 NDAA requires the secretary of defense to conduct an assessment on the viability of a threat information sharing program. The legislation further requires the secretary to determine by the end of FY21 whether or not to establish the program. On the basis of this legislation, the Commission considered the recommendation to be partially implemented, noting that the legislation did not necessarily create the program, and it specified "information sharing" rather than "intelligence sharing." Full implementation of this recommendation, therefore, awaits the required determination by the secretary of defense. Depending on that outcome, further legislation may be needed to fulfill the intent of this recommendation completely.

Recommendation 6.2.2 – Require Threat Hunting on Defense Industrial Base Networks: Like Recommendation 6.2.1, this recommendation was partially authorized by the FY21 NDAA. Section 1739 requires an assessment of the feasibility of implementing a cybersecurity threat hunting program for the defense industrial base. As with Section 1737, the secretary of defense must subsequently determine whether or not to implement the program. If the secretary establishes the program at that point, this recommendation will be considered fully implemented.

Recommendation 6.2.3 – Designate a Threat-Hunting Capability Across the DoD Information Network: Section 1528 of the FY22 NDAA implements this recommendation. While the legislation does not explicitly call for the creation of the force structure element that the Commission recommended, it does require the DoD chief information officer and the commander of U.S. Cyber Command to "facilitate cyber protection team and cybersecurity service provider threat hunting and discovery of novel adversary activity," which meets the intent of this recommendation.[211]

Recommendation 6.2.4 – Assess and Address the Risk to National Security Systems Posed by Quantum Computing: The FY21 NDAA implemented this recommendation through Section 1722, which requires the secretary of defense to "complete a comprehensive assessment of the current and potential threats and risks posed by quantum computing technologies to critical national security systems."[212] As is the case with many recommendations, however, lasting success will depend on the execution of this mandate. As of publication, the report has not yet been received, which is an obvious first requirement for success. Beyond that, lawmakers and national security leaders will need to invest in addressing the recommendations set out in the report.

CSC White Papers

In order to address emerging issues and add greater detail to existing recommendations, the Commission published a series of six white papers in 2020 and 2021:

- May 2020 – Cybersecurity Lessons from the Pandemic
- July 2020 – National Cyber Director[213]
- September 2020 – Growing a Stronger Federal Cyber Workforce
- October 2020 – Building a Trusted ICT Supply Chain
- January 2021 – Transition Book for the Incoming Biden Administration
- December 2021 – Countering Disinformation in the United States

The Transition Book established priorities among existing recommendations but did not put forward new recommendations. The NCD white paper contained one single (existing) recommendation: to establish an NCD. With these two exceptions, the Commission's white papers all recommended numerous additional actions to defend the United States in cyberspace. Implementation rates vary across these papers because of the varied publication dates, but generally, the recommendations laid out in the white papers show strong progress.

White Paper #1: Cybersecurity Lessons From the Pandemic

Cybersecurity Lessons from the Pandemic			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
PAN1.1	Provide State, Local, Tribal, and Territorial Government and Small and Medium-sized Business IT Modernization Grants	Full Implementation via Infrastructure Investment and Jobs Act; Funding Appropriated	
PAN1.2	Pass an Internet of Things Security Law	Partial Implementation via Legislation Passed in FY21 NDAA and Related Executive Order; Further Appropriations Required	
PAN1.3	Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts	Legislation Proposed; Appropriations Required	
PAN1.4	Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns	Legislation Proposed; Appropriations Required	
PAN1.4.1	Establish the Social Media Data and Threat Analysis Center	Authorized via FY21 NDAA; Executive Action Required	

Pandemic Recommendation 1.1 – Provide State, Local, Tribal, and Territorial Government and Small- and Medium-Sized Business Information Technology Modernization Grants: The State and Local Cybersecurity Improvement Act, passed as Sections 70611 and 70612 of the Infrastructure Investment and Jobs Act, implements this recommendation.[214] The law establishes and funds a grant program to address cybersecurity risks and threats to information systems owned and operated by the state, local, tribal, and territorial governments. The program requires grantees to have a cybersecurity plan, and funds can then be used to implement, develop, or revise that plan. Grants can also be used to assist with activities to address imminent cybersecurity threats. Work is still needed to provide similar opportunities for small and medium sized businesses.

Pandemic Recommendation 1.2 – Pass an Internet of Things Security Law: The Internet of Things Cybersecurity Improvement Act of 2020[215] and Section 9204 of the FY21 NDAA set out a path forward for improving the cybersecurity of IoT devices when used by the federal government. Similar legislation does not exist for the national critical infrastructure as a whole.[216] However, the implementation of Executive Order 14028 in 2021 did establish a first step towards providing a framework for such a requirement.[217] Per that order, NIST established recommended criteria — desired outcomes for secure IoT devices —– that could be used to underpin an IoT cybersecurity certification and consumer labeling program.[218] The next step for the administration, which could be taken with or without a congressional mandate but would certainly require an additional appropriation, is to map these criteria to specific standards. In order to fully implement this recommendation, Congress would need to take action to require IoT device manufacturers to meet those standards. Commission staff has drafted model legislation for such a requirement.[219]

Pandemic Recommendation 1.3 – Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts: In 2020, Commission staff proposed legislation that would better enable the government to assist nonprofit organizations that support victims of cybercrime. This concept evolved into a proposal for a nonprofit National Cybercrime Victim Assistance and Recovery Center.[220] The center would provide informational support to small businesses and individuals victimized by cybercrime, including individuals experiencing technology-based stalking and intimate partner abuse. It would also provide information to law enforcement to enable improved support of victims of cybercrime. While the proposal has received support from individual members of Congress, it has yet to be introduced or marked up by the relevant committees.

Pandemic Recommendation 1.4 – Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns: This recommendation was originally proposed as a grant program administered by the Department of Justice in consultation with other departments and agencies to enable nonprofit organizations to identify malign foreign influence campaigns and explain them to the public. Implementing this original recommendation may require authorization of such a program and would necessitate further appropriations. However, the Commission expanded its work on this topic through the publication of a white paper on foreign disinformation in December 2021, which outlines several additional paths for addressing the issues identified in this recommendation.

Pandemic Recommendation 1.4.1 – Establish the Social Media Data and Threat Analysis Center: Section 5323 of the FY20 NDAA authorized the Office of the Director of National Intelligence and the secretary of defense to establish — through a grant or contract — a Social Media Data and Threat Analysis Center.[221] Section 9301 of the FY21 NDAA turned this authorization into a requirement.[222] During his testimony in the Senate, General Nakasone showed his support for the social media data threat analysis center, especially to better understand how adversaries "attempt to garner greater influence."[223] Despite that mandate, there has been no visible executive action or congressional appropriation to indicate that this effort is underway.

White Paper #2: National Cyber Director

National Cyber Director			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
NCD1	Establish a National Cyber Director Position	Legislation Passed in FY21 NDAA; Appropriations Required	

Section 1752 of the FY21 NDAA implemented this recommendation by requiring the establishment of the NCD position. Former National Security Agency Deputy Director and CSC Commissioner John "Chris" Inglis was confirmed to the position on June 16, 2021.[224] The Infrastructure Investment and Jobs Act provided $21 million for the start-up of the office, available through fiscal year 2022.[225] For FY23, the president's budget requested $22 million.[226] In light of the office's growing staff and role, the CSC's congressional commissioners wrote to appropriators in April 2022 to support the president's request for the ONCD for FY23.[227] In light of the sustained progress, this assessment considers the recommendation to be implemented.

White Paper #3: Growing a Stronger Federal Cyber Workforce

Growing a Stronger Federal Cyber Workforce			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
WF1	Establish Leadership and Coordination Structures	Executive Action Required	
WF2	Properly Identify and Utilize Cyber-Specific Occupational Classifications	Executive Action or Legislation Required	
WF3	Develop Apprenticeships	Executive Action Taken; Legislation Introduced	
WF4	Improve Cybersecurity for K-12 Schools	Legislation Passed; Further Legislation or Executive Action Required	
WF5	Provide Work-Based Learning via Volunteer Clinics	Executive Action or Legislation Required	
WF6	Improve Pay Flexibility and Hiring Authorities	Partial Executive Action Taken; Further Executive Action or Legislation Required	
WF7	Incentivize Cyber Workforce Research	Legislation Passed; Appropriations Required	
WF8	Mitigate Retention Barriers and Invest in Diversity in Recruiting	Executive Order Issued; Further Executive Action Required	

Workforce Recommendation 1 – Establish Leadership and Coordination Structures: This recommendation calls for the establishment of two bodies to lead and coordinate cyber workforce development efforts within the federal government: a Cyber Workforce Steering Committee and a Cyber Workforce Coordinating Working Group.[228] The recently published "Workforce Development Agenda for the National Cyber Director" lays out an implementation plan for this recommendation, proposing the purpose and membership of each body.[229]

Workforce Recommendation 2 – Properly Identify and Utilize Cyber-Specific Occupational Classifications: The NIST National Initiative for Cybersecurity Education (NICE) framework is a resource to help employers identify and develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The framework comprises seven categories (high-level groupings of common cybersecurity functions), 33 specialty areas (distinct areas of cybersecurity work), and 52 work roles (groupings of cybersecurity work comprising specific knowledge, skills, and abilities required to perform tasks). When properly utilized by federal workforce hiring managers, the NICE framework can achieve this recommendation., but the NICE office requires additional funding to continue to maintain and improve the framework. This funding is recommended in the FY23 House appropriations. In addition, Section 1118 of the FY22 NDAA calls for updates to the occupational series system "in the fields of software development, software engineering, data science, and data management."[230] Addressing the challenges that confront the federal cyber workforce requires a more targeted response and additional resources.

Workforce Recommendation 3 – Develop Apprenticeships: While elements of this recommendation can be implemented based on existing authorities, a congressional mandate would yield the best results. Senators Hassan and Cornyn introduced the Federal Cybersecurity Workforce Expansion Act, which included a provision for a pilot apprenticeship program at CISA.[231] A version of this proposal was considered for inclusion in the FY22 NDAA but ultimately was not granted the jurisdictional relief. In July 2022, the

ONCD convened a National Cyber Workforce and Education Summit at the White House.[232] In connection, the Departments of Labor and Commerce made a joint announcement launching a 120-Day Cybersecurity Apprenticeship Sprint,[233] supporting the Registered Apprenticeship model to address the cyber industry's talent needs and workforce development.[234]

Workforce Recommendation 4 – Improve Cybersecurity for K-12 Schools: This recommendation focuses not on cybersecurity education but rather on the cybersecurity of the schools themselves. Education facilities are considered a subsector of U.S. critical infrastructure, and thus ensuring their security is a matter of national resilience.[235] To ensure the security of these institutions, Congress passed the K-12 Cybersecurity Act of 2021, which requires CISA to provide a study, recommendations, and a toolkit focused on cybersecurity in schools.[236] The new law partially implements this recommendation; however, further legislative or executive branch action should be considered. An earlier version of the bill included an information exchange, a registry of cyber incidents, and a Technology Improvement Program, which would comprise meaningful steps towards improved cybersecurity for K-12 schools.[237]

Workforce Recommendation 5 – Provide Work-Based Learning via Volunteer Clinics: Existing programs like the Citizen Clinic at the University of California, Berkeley's Center for Long-Term Cybersecurity[238] and the Clinic to End Tech Abuse at Cornell University[239] demonstrate the power of clinics as a teaching and research opportunity as well as a community service in cybersecurity. Encouraging the proliferation of this model to expand educational opportunities and provide services to vulnerable populations would require funding, which could be carried out under existing authorities or required through congressional mandate. In either case, long-term effectiveness would require further appropriations.

Workforce Recommendation 6 – Improve Pay Flexibility and Hiring Authorities: Some progress has been made on parts of this recommendation in the past year. For example, the Office of Personnel Management has established a special salary rate for some cyber positions.[240] However, full implementation of this recommendation, which is closely linked to Recommendation 2 in the white paper on the federal cyber workforce, will require executive action. That executive action may also be supported by congressional mandate, and in one case — the establishment of a new cyber excepted service — it will require authorization.[241] As outlined in detail in the "Workforce Development Agenda for the National Cyber Director," three options could ameliorate some of the challenges to cyber workforce hiring and talent management: 1) expanding cyber hiring authorities beyond existing limitations based on occupational series, 2) creating a new family of occupational classifications, or 3) creating a government-wide cyber excepted service.[242] The first two of these recommendations can be implemented based on existing authorities, but a congressional mandate would help prioritization. The third, which would yield the most effective change, would require new authorities.[243]

Workforce Recommendation 7 – Incentivize Cyber Workforce Research: The passage of the CHIPS and Science Act fully implements this recommendation. Section 10317 establishes a comprehensive cybersecurity workforce data initiative through the National Center for Science and Engineering Statistics (NCSES). It also implements a provision of the FY22 appropriations report, which called for "a study to identify, compile, and analyze existing nationwide data and conduct survey research as necessary to better understand the national cyber workforce.[244] By implementing the NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181), the initiative would collect more consistent and accurate baseline information on the cyber workforce, including its demographics.[245] The initiative represents a starting point for future data-driven policymaking to expand, strengthen, and diversify the cyber workforce. For instance, the data initiative could provide insight into other areas of the cyber workforce, including cybersecurity-related credentials and employment outcomes.[246] The CSC's congressional commissioners further recommended a $4.75 million increase in appropriations for FY23 NDAA for the NCSES to support currently authorized activities to generate increased data on the cybersecurity workforce.

Workforce Recommendation 8 – Mitigate Retention Barriers and Invest in Diversity in Recruiting: Pursuant to the Biden administration's June 25, 2021, Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce,[247] the federal government as a whole is taking steps that indicate this recommendation is seeing some progress towards implementation. The CHIPS and Science Act includes a provision that supports research on the cyber workforce. Section 10315 calls for research and development activities that provide cyber workforce trends, including demographic representation and factors affecting employee recruitment, development, and retention.[248] Similarly, the Cybersecurity Workforce Data Initiative discussed in the prior recommendation would further advance the recommendation by providing metrics to evaluate progress. Successful implementation, however, will require long-term cultural changes in the cybersecurity workforce to foster a more inclusive work environment and the effective use of cyber workforce development research and development data.

White Paper #4: Building a Trusted ICT Supply Chain

Building a Trusted ICT Supply Chain			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
SC1	Develop and Implement an ICT Industrial Base Strategy	Implemented via Executive Order	
SC2	Identify Key ICTs and Materials	Implemented via Executive Order	
SC3	Conduct a Study on the Viability of Critical Technology Clusters and Designate Them	Implemented in FY21 NDAA and CHIPS and Science Act; Funding Appropriated	
SC3.1	Provide Research and Development Funding for Critical Technologies	Implemented via CHIPS and Science Act; Sustained Funding Required	
SC3.2	Incentivize the Movement of Critical Chip and Technology Manufacturing out of China	Partial Implementation via CHIPS and Science Act	
SC3.3	Conduct a Study on a National Security Investment Corporation	Legislation or Executive Action Required	
SC4	Designate Lead Agency for the ICT Supply Chain	Implemented via FY21 NDAA; Funding Appropriated	
SC4.1	Establish a National Supply Chain Intelligence Center	Legislation Proposed	
SC4.2	Fund Critical Technology Security Centers	Legislation Introduced; Funding Appropriated	
SC5	Incentivize Open and Interoperable Standards and Release More Mid-band Spectrum	Legislation Passed; Further Executive Action Required	
SC5.1	Develop a Digital Risk Impact Assessment for International Partners for Telecom Infrastructure Projects	Appropriations Provision Introduced; Further Executive or Legislative Action Required	
SC5.2	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	Legislation Passed; Further Executive and Legislative Action Required	
SC5.3	Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects	Executive Action Required; Legislation Possible	

Supply Chain Recommendation 1 – Develop and Implement an ICT Industrial Base Strategy: The ICT sectoral supply chain assessment required in Section 4 of Executive Order 14017 put implementation of this recommendation in motion.[249] In February 2022, the Departments of Commerce and Homeland Security issued a report responding to this requirement, which outlined key risks and recommendations for securing the ICT supply chain.[250] Coupled with the quadrennial review required by Executive Order 14017, this recommendation is considered fully implemented; however, this determination once again highlights the difference

between the implementation of a recommendation and its long-term success. Maintaining an effective strategy over time will require sustained investment and attention from Congress and the White House.

Supply Chain Recommendation 2 – Identify Key Information and Communication Technologies and Materials: The February 2022 Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry produced by the Departments of Commerce and Homeland Security fully implements this recommendation. The report highlights the hardware manufacturing challenges in the ICT supply chain, honing in on key elements such as circuit boards, fiber optic cables, routers, switches, and servers. It also discusses the software sector, emphasizing issues such as open source software security and firmware risks.[251]

Supply Chain Recommendation 3 – Conduct a Study on the Viability of Critical Technology Clusters and Designate Them: This recommendation is fully implemented through the FY21 NDAA and the passage of the CHIPS and Science Act. The FY21 NDAA created a financial assistance program, a partnership program with the private sector, support for partner and allied supply chains, and centers for research and development, all with the intention of supporting the manufacturing of critical ICT hardware elements like semiconductors domestically and in trusted partner countries.[252] Section 10621 of the CHIPS and Science Act calls for the development of regional technology hubs to bring state, local, tribal, and territorial governments together with universities, the private sector, and others to promote innovation regionally. The Department of Commerce is directed to create 20 "regional technology and innovation hubs" for programs that focus on developing technology, workforce, and innovation capacity with the authorization of $10 billion for fiscal years 2023 through 2027. The provision also designates at least three hubs within the Economic Development Administration's six regions.[253] While the recommendation is fully implemented, further appropriations will be needed to ensure continued effectiveness.

Supply Chain Recommendation 3.1 – Provide Research and Development Funding for Critical Technologies: The passage of the CHIPS and Science Act provides the funding called for in this recommendation. Section 10251 expands awards for Hollings Manufacturing Extension Partnership centers to establish a pilot program that provides services for workforce development, domestic supply chain resilience, and support for small- and medium-sized manufacturers to adopt advanced technology upgrades.[254] As mentioned earlier in Recommendation 4.6.2, the funding for the new Directorate for Technology and Innovation in Sections 10381 and 10389 would support the research and development of critical technologies of this recommendation.[255] Moreover, the Consolidated Appropriations Act, 2022 increased funding around critical issues like artificial intelligence and advanced computing.[256] Accordingly, this recommendation is fully implemented. However, noting that the recommendation calls for not just increased funding but consistent funding, the evaluation of this recommendation may change in the future if the funding increases are not sustained.

Supply Chain Recommendation 3.2 – Incentivize the Movement of Critical Chip and Technology Manufacturing Out of China: The CHIPS and Science Act contains numerous provisions that work towards the larger goal of decreasing material and financial dependence on China for U.S. supply chains. This Act also includes more than $50 billion in appropriations for domestic U.S. chip industry development. This is a significant step towards reducing reliance on chips and technology manufactured out of China. It broadly meets the Commission's proposed path of funding, but it could be improved with a specific grant program to offset the costs to the private sector of relocating manufacturing facilities.

The CHIPS and Science Act contains numerous provisions that work towards the larger goal of decreasing material and financial dependence on China for U.S. supply chains. This Act also includes more than $50 billion in appropriations for domestic U.S. chip industry development. This is a significant step towards reducing reliance on chips and technology manufactured out of China.

Supply Chain Recommendation 3.3 – Conduct a Study on a National Security Investment Corporation: Whether to establish a National Security Investment Corporation or to study its possible impacts, congressional or executive branch action is required to implement this recommendation. The Commission proposed legislation in 2021 that would require a report on a possible corporation. If established, the corporation would not rely on public funding but rather would work to attract private capital and invest it in strategically critical areas.

Supply Chain Recommendation 4 – Designate a Lead Agency for the ICT Supply Chain: Through the FY21 NDAA,[257] DHS was designated as the Sector Risk Management Agency for the information technology sector,[258] fully implementing this recommendation. Executive Order 14017 requires a report on the ICT sector's supply chain, drafted by the Departments of Commerce and Homeland Security, effectively designating those agencies as the lead in that area for the purposes of the executive order.[259] The executive order allows for a vast improvement on the previously siloed efforts by creating an interagency process to evaluate current ICT supply chain conditions. In this whole-of-government approach, the lead agencies collected a variety of data and provided recommendations to mitigate identified vulnerabilities and risks to strengthen the resilience of the ICT supply chain security.[260] Executive Order 13873 directs the Department of Commerce as the lead agency in providing recommendations to protect sensitive personal data in addition to the recommendations for executive and legislative action in addressing risks from using software applications associated with foreign adversaries.[261] CISA requested $18.2 million for SRMA management in the president's budget for fiscal year 2023,[262] an approximately half a million dollar increase from the previous year. However, CISA received a significant increase in its funding through the fiscal year 2022 appropriations bill, which provides $39 million above the request for SRMA activities,[263] including requirements listed under Section 9002 of the FY21 NDAA.[264]

Supply Chain Recommendation 4.1 – Establish a National Supply Chain Intelligence Center: Establishing the National Supply Chain Intelligence Center will require new authorities granted by Congress. Commission staff has proposed model legislation for this center,[265] which would require a report on and plan for consolidating federal supply chain intelligence efforts. Among other activities, the consolidated center would provide ongoing assessment of gaps in intelligence, enhance information sharing with the private sector, and evaluate the effectiveness of current authorities in securing the ICT supply chain.

Supply Chain Recommendation 4.2 – Fund Critical Technology Security Centers: As noted in Recommendation 4.1.1 above, this recommendation is partially implemented as a result of the Infrastructure Investment and Jobs Act, which appropriated $157,500,000 for DHS to "research supporting security testing capabilities relating to telecommunications equipment, industrial control systems, and open source software."[266] Both the House and the Senate have introduced versions of this provision,[267] but it has not yet passed. Accordingly, full implementation of this recommendation will require legislation to provide a clear mandate for the Critical Technology Security Centers.[268]

Supply Chain Recommendation 5 – Incentivize Open and Interoperable Standards and Release More Mid-band Spectrum: Section 90008 of the Infrastructure Investment and Jobs Act tasks DoD with conducting "research and development, engineering studies, economic analyses, activities with respect to systems, or other planning activities to improve efficiency and effectiveness of the spectrum use of the Department of Defense" in order to make more mid-band spectrum available for commercial use and auctions.[269] This legislation partially implements the recommendation as a first step toward releasing the mid-band spectrum. Full implementation will require acting on the findings of the newly authorized studies, and further incentivizing interoperability.

Supply Chain Recommendation 5.1 – Develop a Digital Risk Impact Assessment for International Partners for Telecom Infrastructure Projects: Prior to conferencing the Consolidated Appropriations Act, 2022, the House Committee on Appropriations included a provision for digital risk impact assessments in the report to accompany the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2022.[270] The provision, however, was not included in the final appropriations bill. As such, this recommendation requires further legislative or executive action for implementation.

Supply Chain Recommendation 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: Several provisions are included in the CHIPS and Science Act that align with the overall goal of this recommendation. For example, the CHIPS and Science Act provides the Department of State with $500 million over five years for the America International Technology Security and Innovation Fund. The funding supports the State Department to work with the U.S. Agency for International Development, the Export-Import Bank, and the U.S. International Development Finance Corporation to coordinate with foreign government partners for secure and trusted ICT, semiconductors, and emerging technologies critical to supply chain activities.[271] Related provisions partially implement the rest of this recommendation, and further legislative action may be needed to continue progress. In addition, executive action and appropriations will be needed to make these efforts successful in the long term.

Supply Chain Recommendation 5.3 – Develop a List of Contractors and Vendors Prohibited From Implementing Development Projects: Executive action is required to draw on existing intelligence to determine untrusted contractors and vendors. A legislative mandate for this work would expedite implementation and could help ensure the enforcement of a prohibition.

White Paper #6: Countering Disinformation in the United States

Countering Disinformation in the United States			
Rec. Number	**Recommendation Title**	**Status**	**Assessment**
CD1	Establish a Civic Education Task Force, Enable Greater Access to Civic Education Resources, and Raise Public Awareness	Legislation Introduced; Further Legislation and Appropriations Required	
CD2	Ensure Material Support for Nongovernmental Disinformation Researchers	Appropriations and Authorizing Legislation Required; Executive Action Possible	
CD3	Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public	Legislation Proposed, Appropriations Required	
CD4	Create a Capability within the DHS to Actively Monitor Foreign Disinformation	Legislation Required	
CD5	Create a Grant Program to Equip State and Local Governments	Legislation and Appropriations Required	
CD6	Reform the Foreign Agents Registration Act and Introduce New Federal Communications Commission Regulations	Legislation Required	
CD7	Publish and Enforce Transparency Guidelines for Social Media Platforms	Legislation Mandating Executive Action Required	

Countering Disinformation Recommendation 1 – Establish a Civic Education Task Force, Enable Greater Access to Civic Education Resources, and Raise Public Awareness: Because this white paper was published relatively recently, its recommendations have not yet had the same opportunity for implementation as the rest of the Commission's work. In particular, this timeline limits the legislative progress of the recommendations. Like many recommendations originating in the Countering Disinformation white paper, implementation of this recommendation will require legislative action. Activities like the establishment of a Civic Education Task Force and Clearing House, a student and teacher awards program, a Civic Education Fund, and a National Disinformation Awareness Outreach Program will require new authorizing legislation. Congress can take major steps towards implementing this recommendation by passing the Civics Secures Democracy Act, a bill introduced in both the House and Senate.[272] Even if authorized, civic education activities would need to be funded through appropriations to succeed in the long term.

Countering Disinformation Recommendation 2 – Ensure Material Support for Nongovernmental Disinformation Researchers: Implementation of this recommendation requires authorizing legislation and appropriations for new grant programs administered by the National Science Foundation and by DHS in consultation with the Office of the Director of National Intelligence. Congress can further implement this recommendation by initiating a Congressional Research Service study to help leaders better understand the federal laws that govern social media data and how it is shared. Finally, through executive action or legislative mandate, government leaders can task NIST with improving social media data portability by working with social media companies to establish standard data transfer formats, which would allow researchers to study data across platforms.

Countering Disinformation Recommendation 3 – Provide Grants to Nonprofit Centers to Identify, Expose, and Explain Malign Foreign Influence Campaigns to the American Public: This recommendation mirrors Recommendation PAN1.4, originally introduced in the Commission's May 2020 white paper, "Cybersecurity Lessons from the Pandemic."[273] Implementation of this recommendation will require authorization for a new grant program administered by the Department of Justice, working with other federal departments and agencies, to fund nonprofit researchers working to identify, expose, and explain malign foreign influence campaigns. Commission staff proposed model legislation for this recommendation to accompany the pandemic white paper.[274]

Countering Disinformation Recommendation 4 – Create a Capability Within DHS to Actively Monitor Foreign Disinformation: Implementation of this recommendation will require new authorization to help identify foreign propaganda efforts and disinformation when they occur in the U.S. media environment outside the primary jurisdiction of the intelligence community. Congress can implement this recommendation by authorizing a capability at DHS that can monitor foreign propaganda narratives and present factual information on those topics.

Countering Disinformation Recommendation 5 – Create a Grant Program to Equip State and Local Governments: Implementation of this recommendation will require legislative action and appropriations to authorize and fund a grant program administered by DHS to support state and local governments responding to foreign disinformation. This grant program should be used to help these governments hire staff or procure tools to identify foreign disinformation campaigns and incorporate counter-messaging into public communications.

Countering Disinformation Recommendation 6 – Reform the Foreign Agents Registration Act (FARA) and Introduce New Federal Communications Commission Regulations: Implementation of this recommendation will require amending FARA to remove an exemption to the registration requirement for entities engaged in media production that are registered separately under the Lobbying Disclosure Act. The FARA amendment should also include social media and email in the definition of "informational materials," as previously proposed legislation has detailed.[275] A third beneficial amendment would allow the Department of Justice greater authority to investigate FARA violations. The Disclosing Foreign Influence Act,[276] proposed in 2017, serves as a model for what this legislation could look like. Congress can further implement this recommendation by amending the Telecommunications Act of 1996 to add regulations on domestic media with foreign ownership.[277]

Countering Disinformation Recommendation 7 – Publish and Enforce Transparency Guidelines for Social Media Platforms: This recommendation notably does not require any moderation of content. Rather, it seeks to build transparency around social media companies' content removal policies, advertising, bot labeling, and other activities. To implement this recommendation, Congress should direct the president to develop a plan to draft guidance on these issues, including an entity tasked with taking the lead in developing the guidance.

Further Work by CSC 2.0

The CSC's work as a government entity concluded with the white papers outlined above. However, the CSC 2.0 project has conducted research extending out from the Commission's work, in addition to continuing research and analysis on previous recommendations. Two such reports have been completed.

Cybersecurity in the Water and Wastewater Sector: Water infrastructure in the United States is critical in its own right but is also integral to the functionality of many other critical infrastructure sectors.[278] Nevertheless, cybersecurity for water infrastructure has not received the same attention as comparable sectors like energy or communications. To enhance the security of this sector, CSC 2.0 staff have drafted six legislative proposals:

- Water Proposal 1 – Establish a Water Risk and Resilience Organization[279]
- Water Proposal 2 – Create a Water and Wastewater Infrastructure Cybersecurity Improvement Program[280]
- Water Proposal 3 – Resource and Empower the EPA as the SRMA for the Water Sector[281]
- Water Proposal 4 – Direct More of the EPA's Funding Toward Cybersecurity[282]
- Water Proposal 5 – Establish a Cybersecurity Circuit Rider Program for Rural Water and Wastewater Infrastructure[283]
- Water Proposal 6 – Amend the Clean Water Act to Require Wastewater Systems to Perform Risk and Resilience Assessments[284]

Cyber Workforce Development in the Federal Government: The Commission highlighted a number of challenges in cyber workforce development, as discussed in Recommendation 1.5 and the "Growing a Stronger Federal Cyber Workforce" white paper mentioned above. The CSC 2.0 project addressed a subset of these issues — federal efforts in support of cyber workforce development — and published a memo for the NCD, detailing the actions needed to improve federal efforts in this area.[285]

- Workforce Recommendation 1 – Establish a Process for Ongoing Cyber Workforce Data Collection and Evaluation[286]
  - Recommendation 1.1 – NCD and OPM should provide expanded support for cyber workforce data collection
  - Recommendation 1.2 – NCD should work with leads of federal departments and agencies to ensure accountability for data mandates
  - Recommendation 1.3 – NCD should work with OPM to share data on the federal cyber workforce
  - Recommendation 1.4 – NCD should work with NSF to add to data on the national cyber workforce
- Workforce Recommendation 2 – Establish Leadership and Coordination Structures[287]
  - Recommendation 2.1 – NCD should establish and chair a cyber workforce steering committee
  - Recommendation 2.2 – NCD should establish a cyber workforce coordinating working group
- Workforce Recommendation 3 – Review and Align Cyber Workforce Budgets[288]
  - Recommendation 3.1 – Working with OMB, NCD should review budgets for cyber workforce programs
- Workforce Recommendation 4 – Create a Cyber Workforce Development Strategy for the Federal Government
  - Recommendation 4.1 – NCD should establish a cyber workforce development strategy for the federal government
- Workforce Recommendation 5 – Revamp Cyber Hiring Authorities and Pay Flexibilities Government-Wide
  - Recommendation 5.1 – NCD should work with OPM to modernize cyber-specific coding structures, hiring authorities, and special pay rates government-wide
  - Recommendation 5.2 – NCD should work with OPM to establish a cadre of human resource specialists trained in cyber hiring and talent management
  - Recommendation 5.3 – NCD should work with OPM, OMB, and the appropriations committees to ensure adequate resourcing
- Workforce Recommendation 6 – Recommendations for Congress
  - Recommendation 6.1 – Congress should amend the Federal Cybersecurity Workforce Assessment Act of 2015
  - Recommendation 6.2 – Congress should increase support for the CyberCorps: Scholarship for Service program
  - Recommendation 6.3 – Congress should provide incentives to develop entry–level employees into mid–career talent
  - Recommendation 6.4 – Congress should strive for clarity in roles and responsibilities for cyber workforce development
  - Recommendation 6.5 – Congress should exercise oversight of federal cyber workforce development in each department and agency
  - Recommendation 6.6 – Congress should establish cyber excepted service authorities government-wide
  - Recommendation 6.7 – Congress should expand appropriations for existing efforts in cyber workforce development
- Workforce Recommendation 7 – Recommendations for the Private Sector
  - Recommendation 7.1 – Partners in the private sector should increase their investment in the cyber workforce
  - Recommendation 7.2 – Partners in the private sector should develop shared resources

Conclusion

Since the publication of the first annual assessment in August 2021, Congress and the administration have made substantial progress bolstering U.S. cyber defenses by organizing and resourcing the U.S. government, cooperating with partners and allies, and enhancing collaboration with the private sector. But the work is not done. National cyber resiliency requires long-term investment. Thwarting and punishing malicious cyber actors require persistence. Layered cyber deterrence demands sustained attention. Continuing the important work that the CSC did to draw attention to the challenges and to outline concrete solutions, CSC 2.0 remains committed to supporting efforts to implement the outstanding CSC recommendations and intends to complete the next annual assessment in early fall of 2023.

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. Mark Montgomery, "Congress Invests in National Cyber Resilience but Misses Important Opportunities in the Consolidated Appropriations Act," *Lawfare*, April 1, 2022. (https://www.lawfareblog.com/congress-invests-national-cyber-resilience-misses-important-opportunities-consolidated)

3. House Committee on Appropriations, "Department of Homeland Security Appropriations Bill, 2023," June 24, 2022, page 52. (https://docs.house.gov/meetings/AP/AP00/20220624/114951/HMKP-117-AP00-20220624-SD003.pdf)

4. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 2140. (https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf)

5. U.S. Cyberspace Solarium Commission, "2021 Annual Report on Implementation," August 2021. (https://cybersolarium.org/annual-assessment/2021-annual-report-on-implementation/)

6. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4090. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

7. The recommendations themselves are discussed in more detail in the Commission's final report and accompanying white papers. These publications are available at the CSC 2.0 website, www.cybersolarium.org.

8. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4090. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

9. U.S. Cyberspace Solarium Commission, "Legislative Proposals," July 2020. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Legislative-Proposals.pdf)

10. "Model Legislative Text," *CSC 2.0*, accessed July 22, 2022. (https://cybersolarium.org/model-legislative-text-updated/)

11. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY21," April 3, 2020. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy21/); Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," March 13, 2020. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy21/)

12. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy22/); Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy22/)

13. For further information on the FY21 appropriations process, please see the joint explanatory statements provided by the House Rules Committee. U.S. House of Representatives, Committee on Rules, "Text of Bills for the Week of Dec. 21, 2020," December 21, 2020. (https://docs.house.gov/floor/Default.aspx?date=2020-12-21)

14. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

15. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat. 49.(https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf)

16. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to President Biden Regarding Signaling as a Form of Cyber Deterrence," December 20, 2021. (https://cybersolarium.org/correspondence/letter-to-president-biden-regarding-signaling-as-a-form-of-cyber-deterrence/)

17. Deputy Assistant Secretary of Defense for Cyber Policy Mieke Eoyang, "Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense," *Testimony Before the House Committee on Armed Services*, May 14, 2021. (https://armedservices.house.gov/2021/5/subcommittee-on-cyber-innovative-technologies-and-information-systems-hearing-operations-in-cyberspace-and-building-cyber-capabilities-across-the-department-of-defense); National Cyber Director Chris Inglis, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and James Lewis, "A Conversation with Chris Inglis and Anne Neuberger," *Center for Strategic and International Studies*, October 28, 2021. (https://www.csis.org/events/conversation-chris-inglis-and-anne-neuberger)

18. Tim Starks, "Biden's cyber strategy expected to boost federal role in protecting critical systems from hackers," *CyberScoop*, July 14, 2022. (https://www.cyberscoop.com/national-cyber-strategy-biden-drafting/)

19. Vladimir Soldatkin and Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off-limits,'" *Reuters*, June 16, 2021. (https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/)

20. James Pearson, "Russia downed satellite internet in Ukraine -Western officials," *Reuters*, May 10, 2022. (https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/)

21. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to President Biden Regarding Signaling as a Form of Cyber Deterrence," December 20, 2021. (https://cybersolarium.org/correspondence/letter-to-president-biden-regarding-signaling-as-a-form-of-cyber-deterrence/)

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

23. Ibid., page 4.

24. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to President Biden Regarding Signaling as a Form of Cyber Deterrence," December 20, 2021. (https://cybersolarium.org/correspondence/letter-to-president-biden-regarding-signaling-as-a-form-of-cyber-deterrence/); Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy22/)

25. Office of Representative Mark Takano, Press Release, "Reps. Takano, Casten, Foster, and Beyer Reintroduce the Office of Technology Assessment Improvement and Enhancement Act," February 2, 2022. (https://takano.house.gov/newsroom/press-releases/reps-takano-casten-foster-and-beyer-reintroduce-the-office-of-technology-assessment-improvement-and-enhancement-act)

26. Tonya Riley, "Chris Inglis confirmed as first US national cyber director after Senate vote," *CyberScoop*, June 17, 2021. (https://www.cyberscoop.com/chris-inglis-national-cyber-director-senate-vote/)

27. Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021), §501. (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

28. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2071. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

29. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

30. U.S. Congress, "Joint Explanatory Statement, Division E - Financial Services and General Government Appropriations Act, 2022," March 2022, pages 19–20. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-E.pdf)

31. The White House, "The Budget for Fiscal Year 2023 for the Executive Office of the President," March 2022, page 5. (https://www.whitehouse.gov/wp-content/uploads/2022/03/eop_fy2023.pdf)

32. Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

33. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 1541. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf); National Defense Authorization Act for Fiscal Year 2022, H.R.4350, 117th Congress (2021), §1536. (https://www.congress.gov/bill/117th-congress/house-bill/4350/text)

34. See: U.S. House Committee on the Budget, "Budget Functions," accessed September 8, 2022. (https://budget.house.gov/budgets/budget-functions#050)

35. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act 2022," March 2022, page 137. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

36. U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview: Fiscal Year 2022 Congressional Justification," page 70. (https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency_0.pdf)

37. Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," March 13, 2020. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy21/)

38. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat 1034. (https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf)

39. Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," March 13, 2020. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy21/); Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy22/)

40. Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/wp-content/uploads/2022/05/04.28.21-FY2022-Approps-Letter_House.pdf); Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY21," April 3, 2020. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy21/)

41. Senate Appropriations Committee, "Explanatory Statement for Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2022," page 71. (https://www.appropriations.senate.gov/imo/media/doc/CJSRept_Final.PDF)

42. House Committee on Appropriations "Explanatory Statement, Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2022," July 19, 2021, page 9. (https://www.congress.gov/117/crpt/hrpt97/CRPT-117hrpt97.pdf)

43. Department of Justice, "Federal Bureau of Investigation (FBI): FY 2022 Budget Request at a Glance," page 122. (https://www.justice.gov/jmd/page/file/1399031/download)

44. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022," page 73. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

45. Department of Justice, "Federal Bureau of Investigation (FBI): FY 2022 Budget Request at a Glance," (https://www.justice.gov/jmd/page/file/1489476/download)

46. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4805. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

47. CHIPS and Science Act, Pub. L. No. 117-167, §10316. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

48. 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)

49. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat 2028. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

50. Natalie Alms, "Biden signs bill creating federal cybersecurity rotational program," *FCW*, June 21, 2022. (https://fcw.com/workforce/2022/06/biden-signs-bill-creating-federal-cybersecurity-rotational-program/368424/)

51. Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy22/)

52. Congress appropriated an additional $5 million for FY21 and another $3 million for FY22. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations, 2022," March 2022, page 145. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

53. U.S. National Science Foundation, "FY 2023 Budget Request to Congress," March 28, 2022. (https://www.nsf.gov/about/budget/fy2023/pdf/fy2023budget.pdf)

54. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4805. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

55. U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2022 Budget Submission to Congress," page 38. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf)

56. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022," March 2022, page 13. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

57. U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2023 Budget Submission to Congress," page 37. (https://www.commerce.gov/sites/default/files/2022-03/FY2023-NIST-NTIS-Congressional-Budget-Submission.pdf)

58. U.S. Congressional Budget Office, Cost Estimate, "S. 2775 HACKED Act of 2019," January 31, 2020. (https://www.cbo.gov/system/files/2020-01/s2775.pdf)

59. The White House, Press Release, "Announcement of White House National Cyber Workforce and Education Summit," July 18, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/18/announcement-of-white-house-national-cyber-workforce-and-education-summit/)

60. Aaron Schaffer, "Three takeaways from the Justice Department's cyber review," *The Washington Post*, July 20, 2022. (https://www.washingtonpost.com/politics/2022/07/20/three-takeaways-justice-departments-cyber-review/)

61. David Jones, "White House takes on cyber workforce gap through 120-day apprenticeship sprint," *Cybersecurity Dive*, July 20, 2022. (https://www.cybersecuritydive.com/news/white-house-cyber-workforce-apprenticeship/627705/)

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

63. Executive Assistant Director for Cybersecurity of the Cybersecurity and Infrastructure Security Agency Eric Goldstein, "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks," *Testimony Before the Senate Committee on the Judiciary*, July 27, 2021. (https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks)

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

65. U.S. Senate Committee on Appropriations, "Explanatory Statement for The Homeland Security Appropriations Bill, 2022" page 82. (https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF); U.S. House Committee on Appropriations, "Explanatory Statement, Department of Homeland Security Appropriations Bill, 2022," page 64. (https://www.congress.gov/117/crpt/hrpt87/CRPT-117hrpt87.pdf)

66. Jenna McLaughlin, "White House brings together 30 nations to combat ransomware," *NPR*, October 13, 2021. (https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware)

67. James Pearson, "Russia downed satellite internet in Ukraine -Western officials," *Reuters*, May 10, 2022. (https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10)

68. The document noted that "a single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty." North Atlantic Treaty Organization, "NATO 2022 Strategic Concept," June 29, 2022, page 7. (https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf)

69. CHIPS and Science Act, Pub. L. No. 117-167, §10245. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

70. U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2022 Budget Submission to Congress," June 2021, page 38. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf)

71. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations, 2022," March 2022, page 13. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

72. U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2023 Budget Submission to Congress," March 2022. (https://www.commerce.gov/sites/default/files/2022-03/FY2023-NIST-NTIS-Congressional-Budget-Submission.pdf)

73. Consolidated Appropriations Act, 2022, H.R. 2471, 117th Congress (2021), page 613. (https://www.govinfo.gov/content/pkg/BILLS-117hr2471enr/pdf/BILLS-117hr2471enr.pdf)

74. House Committee on Appropriations, "Explanatory Statement, State, Foreign Operations, and Related Programs Appropriations Bill, 2022," July 6, 2021, page 14. (https://www.congress.gov/117/crpt/hrpt84/CRPT-117hrpt84.pdf)

75. U.S. Department of State, "Congressional Budget Justification: Department of State, Foreign Operations, and Related Programs, Fiscal Year 2023," March 2022, page 162. (https://www.state.gov/wp-content/uploads/2022/03/FY-2023-Congressional-Budget-Justification_Final_03282022.pdf)

76. The White House, "Budget of the U.S. Government, Fiscal Year 2023," March 2022, page 90. (https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf)

77. Note: ALATs are in Bucharest, Romania; Berlin, Germany; Canberra, Australia; Kyiv, Ukraine; London, United Kingdom; Ottawa, Canada; Paris, France; Prague, Czech Republic; Riga, Latvia; Tel Aviv, Israel; The Hague, the Netherlands and Europol/EC3; Copenhagen, Denmark (Stockholm, Sweden suboffice); Seoul, Korea; and Taipei, Taiwan.

78. U.S. House Committee on Appropriations "Explanatory Statement, Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2022," July 19, 2021, page 77. (https://www.congress.gov/117/crpt/hrpt97/CRPT-117hrpt97.pdf)

79. U.S. Department of Justice, "Federal Bureau of Investigation (FBI): FY 2022 Budget Request at a Glance," (https://www.justice.gov/jmd/page/file/1489476/download)

80. 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)

81. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," April 5, 2022. (https://home.treasury.gov/news/press-releases/jy0701)

82. Secretary of State Antony J. Blinken, U.S. Department of State, Press Statement, "Additional Sanctions on Russia's Technology Companies and Cyber Actors" March 31, 2022. (https://www.state.gov/additional-sanctions-on-russias-technology-companies-and-cyber-actors/)

83. Chad P. Bown, "Russia's war on Ukraine: A sanctions timeline," *Peterson Institute for International Economics*, August 15, 2022. (https://www.piie.com/blogs/realtime-economic-issues-watch/russias-war-ukraine-sanctions-timeline)

84. U.S. Department of Justice, "FYs 2022-2026 Strategic Plan," July 1, 2022, page 22. (https://www.justice.gov/doj/book/file/1516901/download)

85. The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/)

86. Eric Tucker, "Microsoft Exchange hack caused by China, US and allies say," *Associated Press*, July 19, 2021. (https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35)

87. Steve Holland and James Pearson, "US, UK: Russia responsible for cyberattack against Ukrainian banks," *Reuters*, February 18, 2022. (https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/)

88. Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, The White House, *Remarks to the Press*, February 18, 2022. (https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/)

89. National Cyber Security Centre, "UK government assess Russian involvement in DDoS attacks on Ukraine," February 18, 2022. (https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine)

90. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Update: Destructive Malware Targeting Organizations in Ukraine," Alert (AA22-057A), April 28, 2022. (https://www.cisa.gov/uscert/ncas/alerts/aa22-057a)

91. Vladimir Soldatkin and Humeyra Pamuk, "Biden tells Putin certain cyberattacks should be 'off-limits'," *Reuters*, June 16, 2021. (https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/)

92. Tamara Keith, "Biden announced a $600 billion global infrastructure program to counter China's clout," *NPR*, June 26, 2022. (https://www.npr.org/2022/06/26/1107701371/biden-announced-a-600-billion-global-infrastructure-program-to-counter-chinas-cl)

93. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

94. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," March 2022, page 64. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

95. Mark Montgomery and Trevor Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure" *Foundation for Defense of Democracies*, November 18, 2021. (https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/); U.S. Environmental Protection Agency, "Fiscal Year 2023, Justification of Appropriation Estimates for the Committee on Appropriations," April 2022, page 10. (https://www.epa.gov/system/files/documents/2022-04/fy-2023-congressional-justification-all-tabs.pdf)

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

97. National Risk Management Act of 2021, S. 1350, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/1350)

98. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

99. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," March 2022, page 63. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

100. Cyber Response and Recovery Act of 2021, S. 1316, 117th Congress. (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/1316)

101. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1267. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

102. U.S. Department of Defense, Press Release, "DOD Details $75 Million Defense Production Act Title 3 Puritan Contract," April 29, 2020. (https://www.defense.gov/News/Releases/Release/Article/2170355/dod-details-75-million-defense-production-act-title-3-puritan-contract/); Executive Order 14001, "On a Sustainable Public Health Supply Chain," January 21, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-a-sustainable-public-health-supply-chain/)

103. Sam Sabin, "The Solarium Commission's most ambitious proposal lacks a game plan," *Politico*, October 18, 2021. (https://www.politico.com/newsletters/weekly-cybersecurity/2021/10/18/the-solarium-commissions-most-ambitious-proposal-lacks-a-game-plan-798275)

104. 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)

105. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2059. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

106. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "CISA Launches New Joint Cyber Defense Collaborative," August 06, 2021. (https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative)

107. Chris Riotta, "CISA expands Joint Cyber Defense Collaborative," *FCW*, April 20, 2022. (https://fcw.com/security/2022/04/cisa-expands-joint-cyber-defense-collaborative/365901/)

108. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "CISA Creates Webpage for Apache Log4j Vulnerability CVE-2021-44228," December 13, 2021. (https://www.cisa.gov/uscert/ncas/current-activity/2021/12/13/cisa-creates-webpage-apache-log4j-vulnerability-cve-2021-44228)

109. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2059. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

110. U.S. Congress, "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)

111. Ibid.,

112. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Storm VIII: National Cyber Exercise," accessed July 25, 2020. (https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise)

113. U.S. Congress, "Joint Explanatory Statement, Division E - Financial Services and General Government Appropriations Act of 2022," March 2022, page 29. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-E.pdf); U.S. Election Assistance Commission, "Fiscal Year 2023 Congressional Budget Justification," 2022. (https://www.eac.gov/sites/default/files/cbj/US_EAC_FY_2023_Congressional_Budget_Justification_508_FINAL.pdf)

114. For the People Act of 2021, H.R. 1, §3002(a) and (g), 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/1/text)

115. Maggie Miller, "Election Commission Approves New Guidelines to Secure, Update Voting Equipment," *The Hill*, February 10, 2021. (https://thehill.com/policy/cybersecurity/538216-election-commission-approves-new-guidelines-to-secure-update-voting)

116. U.S. Congress, "Joint Explanatory Statement, Division E - Financial Services and General Government Appropriations Act of 2022," March 2022, page 31. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-E.pdf)

117. U.S. Congress, "Joint Explanatory Statement, Division E - Financial Services and General Government Appropriations Act of 2022," March 2022, page 4. (https://docs.house.gov/meetings/AP/AP00/20210629/112866/HMKP-117-AP00-20210629-SD002.pdf)

118. U.S. Election Assistance Commission, "Fiscal Year 2023 Congressional Budget Justification," 2022, page 3. (https://www.eac.gov/sites/default/files/cbj/US_EAC_FY_2023_Congressional_Budget_Justification_508_FINAL.pdf)

119. The White House, Press Release, "President Biden's FY 2023 Budget Advances Equity," March 30, 2022. (https://www.whitehouse.gov/omb/briefing-room/2022/03/30/president-bidens-fy-2023-budget-advances-equity/)

120. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Security," June 30, 2022. (https://www.cisa.gov/election-security)

121. "Elections Infrastructure Information Sharing & Analysis Center," *Center for Internet Security*, accessed July 22, 2022. (https://www.cisecurity.org/ei-isac)

122. U.S. Cyberspace Solarium Commission, "Countering Disinformation in the United States," December 2021, pages 17–19. (https://cybersolarium.org/white-papers/countering-disinformation-in-the-united-states/)

123. U.S. Cyberspace Solarium Commission, "Legislative Proposals," July 2020. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Legislative-Proposals.pdf)

124. Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021), §301. (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

125. 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)

126. U.S. Department of Commerce, National Institute of Standards and Technology, "NIST Issues Guidance on Software, IoT Security and Labeling," February 4, 2022. (https://www.nist.gov/news-events/news/2022/02/nist-issues-guidance-software-iot-security-and-labeling)

127. National Defense Authorization Act for Fiscal Year 2022, H.R.4350, 117th Congress (2021), §6461. (https://www.congress.gov/bill/117th-congress/house-bill/4350/text)

128. Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021), §203. (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

129. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

130. Mark Montgomery, "Biden's cyber budget good, but still insufficient to meet the threats." *The Hill*, June 15, 2021. (https://thehill.com/opinion/cybersecurity/558507-bidens-cyber-budget-good-but-still-insufficient-to-meet-the-threats); U.S. Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, "Fiscal Year 2022 Budget Submission to Congress," June 2021, page 38. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf)

131. 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)

132. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations, 2022," March 2022, page 13. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

133. CHIPS and Science Act, Pub. L. No. 117-167, §10223. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

134. U.S. Cyberspace Solarium Commission, "Legislative Proposals," July 2020, page 115. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Legislative-Proposals.pdf)

135. House Committee on Appropriations "Explanatory Statement, Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2022," July 19, 2021, page 27. (https://www.congress.gov/117/crpt/hrpt97/CRPT-117hrpt97.pdf); Senate Appropriations Committee, "Explanatory Statement for Commerce, Justice, Science, and Related Agencies Appropriations Bill of 2022," page 22. (https://www.appropriations.senate.gov/imo/media/doc/CJSRept_Final.PDF)

136. Defense of United States Infrastructure Act of 202, S. 2491, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

137. 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)

138. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

139. U.S. Government Accountability Office, Report to Congressional Committees, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, May 2021, page 8. (https://www.gao.gov/assets/gao-21-477.pdf)

140. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4094. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

141. U.S. Government Accountability Office, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," May 2021, page 4. (https://www.gao.gov/assets/gao-21-477.pdf)

142. U.S. Government Accountability Office, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 2022. (https://www.gao.gov/assets/gao-22-104256.pdf)

143. Federal Information Security Modernization Act of 2021, S. 2902, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/2902?s=1&r=1)

144. Federal Information Security Modernization Act of 2022, H.R. 6497, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/house-bill/6497)

145. 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)

146. U.S. Securities and Exchange Commission, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," 87 *Federal Register* 13524, March 9, 2022. (https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business); Jiwon Ma and Mark Montgomery, "Corporate Transparency Would Reduce Systemic Cyber Risks," *Bloomberg Law*, April 4, 2022. (https://news.bloomberglaw.com/securities-law/corporate-transparency-would-reduce-systemic-cyber-risks)

147. U.S. House Committee on Appropriations "Explanatory Statement, Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2022," July 19, 2021, page 27. (https://www.congress.gov/117/crpt/hrpt97/CRPT-117hrpt97.pdf); U.S. Senate Committee on Appropriations, "Explanatory Statement for Commerce, Justice, Science, and Related Agencies Appropriations Bill of 2022," page 22. (https://www.appropriations.senate.gov/imo/media/doc/CJSRept_Final.PDF)

148. 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)

149. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

150. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4777. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

151. International Cybercrime Prevention Act, S. 3288, 115th Congress (2018). (https://www.congress.gov/bill/115th-congress/senate-bill/3288/text)

152. U.S. Department of Justice, Press Release, "Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)," April 6, 2022. (https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation)

153. Joe Warminsky, "US says it disrupted Russian botnet 'before it could be weaponized,'" *CyberScoop*, April 6, 2022. (https://www.cyberscoop.com/russian-botnet-disrupted-garland-doj/)

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

155. Ibid.

156. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 1843. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

157. CHIPS and Science Act, Pub. L. No. 117-167, §10224. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

158. Ibid., §10253.

159. See, for example: U.S. Congress, "Joint Explanatory Statement, Division C Part 2 - Department of Defense Appropriations Act, 2022," March 2022. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-C_Part2.pdf)

160. CHIPS and Science Act, Pub. L. No. 117-167, §10381. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

161. Ibid., §10389.

162. U.S. Senate Committee on Appropriations, "Explanatory Statement for Financial Services and General Government Appropriation Bill, 2022," page 42. (https://www.appropriations.senate.gov/imo/media/doc/FSGGRPT_FINAL2.PDF); U.S. House Committee on Appropriations, "Explanatory Statement, Financial Services and General Government Appropriations Bill, 2022," July 1, 2021, page 54. (https://www.congress.gov/117/crpt/hrpt79/CRPT-117hrpt79.pdf)

163. The White House, "The Budget for Fiscal Year 2023 for the Department of the Treasury," March 2022, page 981. (https://www.whitehouse.gov/wp-content/uploads/2022/03/tre_fy2023.pdf)

164. Financial Services and General Government Appropriations Act, 2023, H.R. 8254, 117th Congress (2022), page 49. (https://www.congress.gov/bill/117th-congress/house-bill/8254/text)

165. National Security Telecommunications Advisory Committee, "NSTAC Report to the President on a Cybersecurity Moonshot," November 14, 2018, ES-1, 5. (https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf)

166. 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/)

167. U.S. Cyberspace Solarium Commission, "Legislative Proposals," July 2020, page 141. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Legislative-Proposals.pdf)

168. CHIPS and Science Act, Pub. L. No. 117-167, §10375. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

169. American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2022). (https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152ih.pdf)

170. For example, see: "Senate Homeland Security Hearing on Colonial Pipeline Cyber Attack," *C-Span*, June 8, 2021. (https://www.c-span.org/video/?512247-1/senate-homeland-security-hearing-colonial-pipeline-cyber-attack)

171. U.S. Congress, "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)

172. Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

173. "Legislative Proposals Remaining from March 2020 Report," *CSC 2.0*, accessed July 22, 2022. (https://cybersolarium.org/model-legislative-text-updated/)

174. Ibid.

175. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4094. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

176. National Defense Authorization Act for Fiscal Year 2022, H.R.4350, 117th Congress (2021), §150. (https://www.congress.gov/bill/117th-congress/house-bill/4350/text)

177. Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021), §202. (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

178. 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)

179. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," March 2022, pages 57–58. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

180. Joseph Marks, "Vast Majority of our Network Cyber Experts Favor Mandates to Report Hacks," *The Washington Post*, December 6, 2021. (https://www.washingtonpost.com/politics/2021/12/06/vast-majority-our-network-cyber-experts-favor-mandates-report-hacks/)

181. 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)

182. U.S. Congress, "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)

183. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4120. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

184. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2021," 117th Congress (2021), page 51. (https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-F.pdf)

185. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," 117th Congress (2022), page 59. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

186. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Budget Overview: Fiscal Year 2022 Congressional Justification," 2021, page 68. (https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency_0.pdf)

187. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," accessed on July 25, 2022. (https://www.cisa.gov/jcdc)

188. U.S. Department of Homeland Security, "FY 2023 Budget in Brief," March 24, 2022, page 64. (https://www.dhs.gov/sites/default/files/2022-03/22-%201835%20-%20FY%202023%20Budget%20in%20Brief%20FINAL%20with%20Cover_Remediated.pdf)

189. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4118. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

190. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2039. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

191. Ibid., 135 Stat. 2032.

192. Ibid., 135 Stat. 2064.

193. General Paul Nakasone, "Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense," *Testimony Before the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems*, April 5, 2022. (https://armedservices.house.gov/2022/4/subcommittee-on-cyber-innovative-technologies-and-information-systems-hearing-operations-in-cyberspace-and-building-cyber-capabilities-across-the-department-of-defense)

194. Mark Pomerleau, "Cyber Command's Force Is Growing in Part, to Support Space," *FedScoop*, April 8, 2022. (https://www.fedscoop.com/cyber-commands-force-is-growing-in-part-to-support-space/)

195. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2028. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

196. U.S. Cyber Command, "US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise," April 15, 2021. (https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/)

197. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

198. The White House, "Fact Sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment," June 26, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/)

199. G7 Germany, "G7 Leaders' Communique," June 28, 2022. (https://www.governo.it/sites/governo.it/files/2022-06-28-abschlusserklaerung-eng-web-data.pdf)

200. North American Treaty Organization, "NATO 2022 Strategic Concept," June 29, 2022, page 7. (https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf)

201. Mark Pomerleau, "Cyber Command has Deployed to Nations 27 Times to Help Partners Improve Cybersecurity," *FedScoop*, March 4, 2022. (https://www.fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/)

202. General Paul Nakasone, "Posture Statement of Gen. Paul M. Nakasone, Commander, U.S. Cyber Command Before the 117th Congress," *Testimony Before the Senate Committee on Armed Services*, April 5, 2022. (https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf)

203. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 133 Stat. 1747. (https://www.congress.gov/bill/116th-congress/senate-bill/1790/text)

204. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4119. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

205. Civilian Cybersecurity Reserve Act, S.1324, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/senate-bill/1324)

206. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2028. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

207. Section 1640 of the FY18 NDAA established the Strategic Cybersecurity Program. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1745. (https://www.congress.gov/bill/115th-congress/house-bill/2810/text?r=278)

208. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2093. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

209. 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)

210. 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/)

211. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 2046. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

212. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4109. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

213. During its tenure, the CSC chose not to release this white paper publicly.

214. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1272. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

215. IoT Cybersecurity Improvement Act of 2020, H.R. 1668, 116th Congress (2020). (https://www.congress.gov/bill/116th-congress/house-bill/1668)

216. In some cases, individual states have implemented such provisions. See, for example: Information Privacy: Connected Devices, Senate Bill no. 327, General Assembly of California, 2018. (https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327)

217. 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)

218. U.S. Department of Commerce, National Institute of Standards and Technology, "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products," February 4, 2022. (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

219. U.S. Cyberspace Solarium Commission, "Cybersecurity Lessons from the Pandemic: CSC White Paper #1," May 2020, page 14. (https://cybersolarium.org/white-papers/cybersecurity-lessons-from-the-pandemic/)

220. "Pandemic White Paper Model Legislative Texts," *CSC 2.0*, accessed August 31, 2022. (https://cybersolarium.org/model-legislative-text-updated/#Pandemic-White-Paper-Model-Legislative-Texts)

221. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 133 Stat. 2130. (https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf)

222. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4801. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

223. Martin Matishak, "Around the Horn with the Head of U.S. Cyber Command," *The Record*, April 5, 2022. (https://therecord.media/around-the-horn-with-the-u-s-cyber-command-chief/)

224. Eric Geller, "Senate Confirms Chris Inglis as Biden's Top Cyber Adviser," *Politico*, June 17, 2021. (https://www.politico.com/news/2021/06/17/senate-confirms-chris-inglis-cyber-495075)

225. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1381–1382. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

226. The White House, "The Budget for Fiscal Year 2023 for the Executive Office of the President," page 5. (https://www.whitehouse.gov/wp-content/uploads/2022/03/eop_fy2023.pdf)

227. Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. Senate Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-senate-appropriations-committee-regarding-appropriations-requests-for-fy22/); Representative Jim Langevin and Representative Mike Gallagher, Cyberspace Solarium Commission, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY22," April 28, 2021. (https://cybersolarium.org/correspondence/letter-to-the-u-s-house-appropriations-committee-regarding-appropriations-requests-for-fy22/)

228. U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020, page 8. (https://cybersolarium.org/wp-content/uploads/2022/05/Growing-a-Stronger-Federal-Workforce-CSC-White-Paper-3.pdf)

229. Laura Bate and Mark Montgomery, "Workforce Development for the National Cyber Director," *CSC 2.0*, June 2022 (https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf)

230. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 1956. (https://www.congress.gov/117/plaws/publ81/PLAW-117publ81.pdf)

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

232. The White House, Press Release, "Announcement of White House National Cyber Workforce and Education Summit," July 18, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/18/announcement-of-white-house-national-cyber-workforce-and-education-summit/)

233. U.S. Department of Labor, Press Release, "US Departments of Labor, Commerce Announce 120-Day Cybersecurity Apprenticeship Sprint to Promote Registered Apprenticeships," July 19, 2022. (https://www.dol.gov/newsroom/releases/osec/osec20220719)

234. "Cybersecurity Apprenticeship Sprint," *Apprenticeship.gov*, accessed July 26, 2022. (https://www.apprenticeship.gov/cybersecurity-apprenticeship-sprint)

235. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Government Facilities Sector," accessed July 26, 2022. (https://www.cisa.gov/government-facilities-sector)

236. K-12 Cybersecurity Act of 2021, S. 1917, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/1917/text)

237. Enhancing K-12 Cybersecurity Act, H.R. 4005, 117th Congress (2021). (http://www.congress.gov/bill/117th-congress/house-bill/4005/text)

238. University of California, Berkeley, Center for Long-Term Cybersecurity, Press Release, "CLTC Launches Cybersecurity 'Citizen Clinic,'" October 24, 2018. (https://cltc.berkeley.edu/2018/10/24/cltc-launches-cybersecurity-citizen-clinic/)

239. "Center to End Tech Abuse," *Cornell University*, accessed July 26, 2022. (https://www.ceta.tech.cornell.edu/)

240. Office of Personnel Management, "Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals," accessed August 31, 2022. (https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf)

241. For model legislation for this proposal, see: "Federal Cyber Excepted Service," *CSC 2.0*, accessed September 8, 2022. (https://cybersolarium.org/wp-content/uploads/2022/06/Federal-Cyber-Excepted-Service.pdf)

242. U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020, pages i–ii. (https://cybersolarium.org/wp-content/uploads/2022/05/Growing-a-Stronger-Federal-Workforce-CSC-White-Paper-3.pdf)

243. For model legislation for these new authorities, see: "Workforce Model Legislative Texts," *CSC 2.0*, accessed August 31, 2022. (https://cybersolarium.org/model-legislative-text-updated/#Workforce-Model-Legislative-Texts)

244. U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations, 2022," March 2022, page 142. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

245. For further reading on demographic data in the cybersecurity workforce, see: Irving Lachow, "Equity and Diversity in the Nation's Cyber Workforce: Policy Recommendations for Addressing Data Gaps," *Center for Strategic and International Studies*, April 5, 2022. (https://www.csis.org/analysis/equity-and-diversity-nations-cyber-workforce-policy-recommendations-addressing-data-gaps)

246. CHIPS and Science Act, Pub. L. No. 117-167, §10317. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

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

248. CHIPS and Science Act, Pub. L. No. 117-167, §10315. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

249. 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/)

250. 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)

251. 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)

252. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4846–4852 and 4854–4860. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

253. CHIPS and Science Act, Pub. L. No. 117-167, §10621. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

254. Ibid., §10251.

255. Ibid., §§10381 and 10389.

256. See, for example, the increases to research initiatives in these areas in: U.S. Congress, "Joint Explanatory Statement, Division C, Part 2 - Department of Defense Appropriations Act, 2022," March 2022. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-C_Part2.pd). See also the increases for advanced communications research at the National Telecommunications and Information Administration in: U.S. Congress, "Joint Explanatory Statement, Division B - Commerce, Justice, Science, and Related Agencies Appropriations, 2022," March 2022, pages 9–11. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

257. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768–4773. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

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

259. 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/)

260. U.S. Department of Homeland Security, 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)

261. Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries," June 9, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/)

262. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Budget Overview Fiscal Year 2022 Congressional Justification," 2021, page 8. (https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency_0.pdf#page=8)

263. U.S. Congress, "Joint Explanatory Statement, Division F - Department of Homeland Security Appropriations Act, 2022," March 2022, page 64. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf#Page=64)

264. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 4768. (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

265. "Legislative Proposals Remaining from March 2020 Report," *CSC 2.0*, accessed July 22, 2022. (https://cybersolarium.org/model-legislative-text-updated/#Proposals-Remaining-from-March-2020-report)

266. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 1388. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

267. National Defense Authorization Act for Fiscal Year 2022, H.R.4350, 117th Congress (2021), §6461. (https://www.congress.gov/bill/117th-congress/house-bill/4350/text); Defense of United States Infrastructure Act of 2021, S. 2491, 117th Congress (2021), §203. (https://www.congress.gov/bill/117th-congress/senate-bill/2491)

268. Model text for this provision is available at: "Legislative Proposals Remaining from March 2020 Report," *CSC 2.0*, accessed July 22, 2022. (https://cybersolarium.org/model-legislative-text-updated/)

269. Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 429. (https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf)

270. U.S. House of Representatives, "Department of State, Foreign Operations, and Related Programs Appropriations Bill, 2022," 2021. (https://www.congress.gov/117/crpt/hrpt84/CRPT-117hrpt84.pdf)

271. CHIPS and Science Act, Pub. L. No. 117-167, 136 Stat. 1372. (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf)

272. Civics Secures Democracy Act of 2021, H.R. 1814, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/1814/actions); Civics Secures Democracy Act, S. 879, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/879)

273. U.S. Cyberspace Solarium Commission, "Cybersecurity Lessons from the Pandemic," June 2, 2020. (https://cybersolarium.org/white-papers/cybersecurity-lessons-from-the-pandemic/)

274. Ibid.

275. See: Foreign Agents Registration Modernization and Enforcement Act, H.R. 2811, 115th Congress (2017). (https://www.congress.gov/bill/115th-congress/house-bill/2811); Foreign Agents Registration Modernization and Enforcement Act, S.625, 115th Congress (2017). (https://www.congress.gov/bill/115th-congress/senate-bill/625)

276. Disclosing Foreign Influence Act, S. 2039, 115th Congress (2017). (https://www.congress.gov/bill/115th-congress/senate-bill/2039/text)

277. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. (https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg56.pd)

278. Mark Montgomery and Trevor Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure" *Foundation for Defense of Democracies*, November 18, 2021. (https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/)

279. "Water 1 - Establish a Water Risk and Resilience Organization," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_1.pdf)

280. "Water 2 - Water and Wastewater Infrastructure Cybersecurity Improvement Program," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_2.pdf)

281. "Water 3 - Resource and Empower the EPA as the SRMA for the Water Sector," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_3.pdf)

282. "Water 4 - Direct More of the EPA's Funding Toward Cybersecurity," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_4.pdf)

283. "Water 5 - Cybersecurity Circuit Rider Program for Rural Water and Wastewater Infrastructure," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_5.pdf)

284. "Water 6 - Amend the Clean Water Act to Require Wastewater Systems to Perform Risk and Resilience Assessments," *CSC 2.0*, May 2022. (https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_Water_6.pdf)

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

286. "Federal Cybersecurity Workforce Data Collection," *CSC 2.0*, June 2022. (https://cybersolarium.org/wp-content/uploads/2022/06/Federal-Cybersecurity-Workforce-Data-Collection.pdf)

287. "Federal Cyber Workforce Development Institute," *CSC 2.0*, June 2022. (https://cybersolarium.org/wp-content/uploads/2022/06/Federal-Cyber-Workforce-Development-Institute.pdf)

288. "Federal Cyber Expected Service," *CSC 2.0*, June 2022. (https://cybersolarium.org/wp-content/uploads/2022/06/Federal-Cyber-Excepted-Service.pdf)

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.

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

On behalf of the entire staff that contributes to the CSC 2.0 project, the authors would like to thank the co-chairs and distinguished advisors for entrusting us with the continuation of the work of the Cyberspace Solarium Commission. The Commission was effective because of their thought leadership and determination to advance effective policy solutions. We are grateful for the willingness of the CSC 2.0 co-chairs, distinguished advisors, and senior advisors to share expertise and offer advice on this annual assessment. We also owe a debt of gratitude to the former staff of the Commission, particularly Laura Bate, who contributed substantial research to this assessment both as staff to the Commission and as an advisor to the CSC 2.0 project prior to joining the U.S. government. We would also like to thank Annie Fixler, who steers many CCTI projects to fruition, coordinating various moving pieces while setting standards of excellence for the research in the CSC 2.0 assessment report. We are also grateful to Trevor Logan and Erik Thomas for helping verify many of the data points in this report, and to John Hardie 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: October 19, 2021 - Auburn, AL, USA: McCrary Institute, Public Private Partnerships in Cybersecurity (Julie Bennett/Auburn University Media Production Group)

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

About CSC 2.0

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

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

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

Co-Chairmen

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

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, Chairman, President, and Chief Executive Officer of Southern Company

James R. "Jim" Langevin, 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

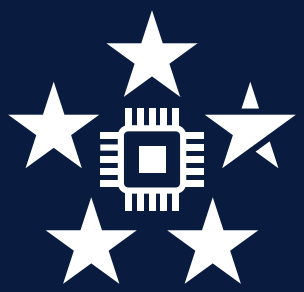
Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, 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