TRANSITION BOOK FOR THE INCOMING BIDEN ADMINISTRATION

CSC White Paper #5

JANUARY 2021

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN
Senator Angus King (I-Maine)
Representative Mike Gallagher (R-Wisconsin)

CONTENTS

INTRODUCTION AND COMMISSION BACKGROUND

The digital connectivity that has brought economic growth, technological dominance, and an improved quality of life to nearly every American has also created a strategic dilemma. The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide. Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing. For more than 20 years, nation-states and non-state actors have leveraged cyberspace to subvert American power, American security, and the American way of life. The perpetrators of these cyberattacks exploited weakness in both systems and strategy and assessed that their forays damaged the United States without triggering any significant retaliation. American restraint was met with unchecked predation.[1] The U.S. Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to address these challenges and "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."[2]

To meet its mandate, the CSC produced a final report, published in March 2020, outlining a strategic approach and over 80 recommendations for the U.S. government. In the development of the final report, task forces met with more than 300 stakeholders from industry; academia; federal, state, and local governments; international organizations; and think tanks, and they stress-tested their recommendations through a series of red team reviews and a scenario-based event. Following the Solarium event, the Commissioners assessed each strategy and its supporting policy recommendations, providing formal feedback. The staff tabulated this feedback and used the insights and guidance to further refine the recommendations.

In the months since the launch of the final report, 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 four white papers with new and updated recommendations: they addressed lessons on cybersecurity from the pandemic, details on the national cyber director recommendation, a framework for a cybersecurity workforce development strategy, and proposals on how to secure America's information and communications technology (ICT) supply chains. Many of the Commission's critical recommendations have been enacted in legislation, but there is still more work to be done to meet the urgent challenges facing our nation, and much can be achieved through coordinated and thoughtful executive action.

This white paper is intended to provide a guide for the incoming Biden-Harris administration, identifying possible early policy achievements and suggesting priorities for action over the coming months and years. The recommendations contained in this booklet are discussed in more detail in the Commission's final report and accompanying white papers.[3]

EARLY PRIORITIES: FIRST 100 DAYS

Within the first 100 days of taking office, the Biden-Harris administration can set in motion three processes that will elevate cybersecurity as an imperative across the government and put the United States on a path toward reducing the probability and impact of cyberattacks against it.

1. ESTABLISH THE OFFICE OF THE NATIONAL CYBER DIRECTOR

Numerous commissions, initiatives, and studies have recommended a more robust and institutionalized national-level mechanism for coordinating cybersecurity and associated emerging technology issues, and for overseeing the executive branch's development and implementation of an integrated national cybersecurity strategy. As emerging technology- and cyberspace-related issues become more complex—and consequently become a greater threat to U.S. national security—the President's need for sound advice and timely options will be increasingly critical.

To ensure strong, stable, and expert-led cybersecurity leadership in the White House, ***the Biden-Harris administration should nominate a National Cyber Director, for Senate confirmation, within its first 30 days, and begin building the Office of the National Cyber Director***. The FY2021 National Defense Authorization Act (NDAA) established the National Cyber Director and the Office of the National Cyber Director.[4] The National Cyber Director, situated within the Executive Office of the President, is a Senate-confirmed advisor to the President who fills several important roles, including

1. Acting as the President's principal advisor on cybersecurity and associated emerging technology issues;

2. Leading the development of a National Cyber Strategy and ensuring its implementation across departments and agencies, including reviewing agency budgets and ensuring the effective integration of interagency efforts;

3. Overseeing and coordinating federal government activities to defend the United States in the face of adversary cyber operations, including serving as a primary point of contact with the private sector as well as with state, local, tribal, and territorial entities; and

4. Convening and coordinating Cabinet-level or National Security Council Principals Committee–level meetings and associated preparatory meetings, with concurrence from the National Security Advisor or the National Economic Advisor.

As part of standing up the Office of the National Cyber Director, the Biden-Harris administration should set out the relationships, roles, and responsibilities between the Deputy National Security Advisor for Cyber and Emerging Technology and the National Cyber Director within the White House. The Commission believes these roles are complementary and collectively ensure the National Security Advisor is well served in the consideration and execution of a whole-of-nation strategy supporting national security objectives. The Deputy National Security Advisor should represent the interests and capabilities of departments and agencies executing Title 10 and Title 50 cyber operations and provide a critical liaison between them and the National Security Council, and ensure that the National Cyber Director has full visibility into the cyber activities of those entities. The National Cyber Director should focus on coordinating, supporting, and deconflicting whole-of-nation cybersecurity and defensive cyber efforts led by executive branch agencies. In so doing, the National Cyber Director should lead White House engagement with the private sector to build trust and advance shared interests and should represent the administration on cyber issues both at home and abroad. To complement this effort, the Biden-Harris administration

should review and update Presidential Policy Directive 41 to designate the National Cyber Director as the lead coordinator for federal cyber incident response efforts and establish the National Cyber Director's responsibility to provide comprehensive recommended policies and actions to the National Security Advisor. Similarly other rulemaking processes that have a bearing on cybersecurity should also be updated to include National Cyber Director integration.

2. DEVELOP AND PROMULGATE A NATIONAL CYBER STRATEGY

Once the National Cyber Director is in place, ***the Biden-Harris administration should begin the process of developing and promulgating a new National Cyber Strategy for the United States of America***. The 2018 National Cyber Strategy was the first U.S. national cybersecurity strategy issued in nearly 15 years and only the second in the nation's history.

Any effective strategy for cyberspace will require a coordinated effort across the multiple stakeholders within the federal government, state and local governments, and the private sector that are all responsible for securing and defending the United States in this domain. Therefore, the strategy must explicitly align and synchronize stakeholder strategic objectives, identify lines of effort to put the strategy into operation, clarify what priority should be given to various efforts, and articulate common principles of risk. Furthermore, the strategy should integrate the concept of "defend forward," which currently anchors the Department of Defense's 2018 Cyber Strategy, into the broader U.S. cyber strategy. The strategy should make defend forward an integral part of a comprehensive approach that encompasses the employment not just of strictly military capabilities but of all instruments of national power: these include economic efforts, law enforcement activities, diplomatic tools, and signals directed to both allies and adversaries.

The new National Cyber Strategy should articulate a framework for successfully disrupting and deterring our adversaries from ever undertaking significant cyberattacks through layered cyber deterrence and should set forth ways and means of (1) shaping adversary behavior, (2) denying adversaries benefits, and (3) imposing costs on adversaries. While deterrence is an enduring American strategy, there are two factors that make layered cyber deterrence bold and distinct. First, the approach prioritizes deterrence by denial, specifically by increasing the defense and security of cyberspace through resilience and public- and private-sector collaboration, reducing the vulnerabilities adversaries can target. Second, the strategy incorporates the concept of "defend forward" discussed above.

Finally, the new strategy should incorporate a multitiered signaling strategy and a new declaratory policy for the United States. The signaling strategy should articulate a framework that clearly communicates when and under what conditions the U.S. government will voluntarily disclose cyber operations and campaigns in order to signal capability and intent to various audiences. The declaratory policy should clearly state that the United States will respond using cyber and non-cyber capabilities to counter and to impose costs on adversary cyber campaigns below a use-of-force threshold. Essentially, the U.S. government should publicly declare that it will defend forward and should couple its declaration with decisive and consistent action across all elements of national power.

3. IMPROVE THE COHERENCE AND IMPACT OF EXISTING GOVERNMENT CYBERSECURITY EFFORTS AND FURTHER STRENGTHEN PARTNERSHIPS WITH THE PRIVATE SECTOR

While private-sector entities and state, local, tribal, and territorial governments are responsible for the defense and security of their networks, the U.S. government must bring to bear its unique authorities and resources, as well as diplomatic, economic, military, law enforcement, and intelligence capabilities, to support these actors in their defense efforts. In addition, as the SolarWinds incident has shown, federal government departments and agencies must bolster their capabilities both to prevent cyber incidents and to identify, detect, and effectively respond to them when they do occur. To improve the ability

of the U.S. government both to defend itself in cyberspace and to work collaboratively with private-sector entities and other key players, the Biden-Harris administration should strengthen the integrated cyber center within the Cybersecurity and Infrastructure Security Agency (CISA) and build the Joint Cyber Planning Office.

A. Review Federal Agency Cybersecurity Budgets for FY2022 Appropriations

The massive SolarWinds hack has laid bare the urgent need to improve cybersecurity within federal departments and agencies and within federal cybersecurity centers. ***Through the National Cyber Director, the Biden-Harris administration should conduct a 90-day review of federal agency cybersecurity budgets***. The budget review should identify existing budgets for cybersecurity operations and programming within federal departments and agencies and should assess the difference between the amount currently allocated and the amount needed to achieve legally mandated missions. It should examine agency enterprise cybersecurity and Federal Information Security Management Act budgets as well as budgets for agency cybersecurity programming. Also falling under the review's scope should be budgets needed for agencies to carry out new mandates, including those of the Cybersecurity and Infrastructure Security Agency as created by the FY2021 NDAA, to (1) hunt for and identify threats and vulnerabilities within federal information systems; (2) provide services, functions, and capabilities to assist federal agencies; and (3) deploy, operate, and maintain secure technology platforms and tools, including networks and common business applications. Further, the review should evaluate whether the existing budgets of Sector Risk Management Agencies are adequate in light of the new requirements that accompany the codification of their roles in the FY2021 NDAA.[5]

B. Strengthen an Integrated Cyber Center within CISA

The FY2021 NDAA requires a review of federal cyber centers and the strengthening of the nascent integrated cyber center within CISA. To truly operationalize cybersecurity collaboration with the private sector, ***the Biden-Harris administration should implement this mandate to strengthen the integrated cyber center within CISA, designate it the lead cybersecurity center for asset response activities, and improve its connections with other key federal and private cyber and cybersecurity centers.*** Doing so will ensure that the systems, processes, and human element of collaboration and integration are fully brought to bear in operational support of the critical infrastructure cybersecurity and resilience mission. CISA's cyber mission, which was initially conceptualized through a national cybersecurity and communications integration center, is envisioned to be the U.S. government's primary coordinating body charged with forging whole-of-government, public-private collaboration during cybersecurity operations. However, CISA has been institutionally limited in its ability to fully carry out this mission, hindered by inadequate facilities and personnel policies, insufficient resources, lack of buy-in from other federal departments and agencies, ambiguity from Congress on its role and position in relation to other agencies, and inconsistent support to and integration with the private sector.

C. Create a Joint Cyber Planning Office within CISA

In addition to calling for a stronger integrated cyber center to carry out real-time cyber defense, the FY2021 NDAA mandates the creation of a Joint Cyber Planning Office (JCPO) within CISA to formulate plans and orchestrate exercises.[6] The bill funding the Department of Homeland Security in FY2021 provides $10.568 million for that purpose.[7] ***The Biden-Harris administration should establish a JCPO under CISA to coordinate cybersecurity planning and readiness across the federal government and between the public and private sectors in order to prepare for significant cyber incidents and malicious cyber campaigns.*** Taking strategic guidance from a national cyber strategy overseen by the National Cyber Director, the JCPO should be composed of a central planning staff and representatives from the integrated cyber center, as well as from other federal agencies that wield operational cyber capabilities and/or authorities in defense of critical infrastructure. The JCPO should be designed to facilitate comprehensive planning of defensive, non-intelligence cybersecurity campaigns across agencies, integrate these planning efforts with those of the private sector, and be managed and hosted by CISA.

D. Set Expectations and Responsibilities for Sector Risk Management Agencies

The FY2021 NDAA codifies sector-specific agencies in law as Sector Risk Management Agencies (SRMAs), setting baseline expectations and responsibilities for these vital agencies that liaise with critical infrastructure sectors. This is a crucial first step in building government structures that enable more mature government support to the private sector on cybersecurity. ***The Biden-Harris administration should implement the provisions in the FY2021 National Defense Authorization Act regarding Sector Risk Management Agencies and increase SRMA capacity to meet the threat by rewriting Presidential Policy Directive 41 and outlining expectations and responsibilities for SRMAs.*** It is crucial that the Biden-Harris administration does this in its first 100 days so that SRMAs can use the remainder of the year to understand their new responsibilities and submit budget requests aligned with those responsibilities.

PRIORITIES FOR EXECUTIVE ACTION BEYOND 100 DAYS

With leadership and coordination structures established in the White House and a national cybersecurity strategy set in place in the first 100 days, seven key priorities should shape the focus of the Biden-Harris administration on cybersecurity issues over the remainder of its term.

1. RESTORE AMERICAN INTERNATIONAL CYBER LEADERSHIP

The United States has watched its strength as an international leader on cybersecurity issues erode. Although American diplomats have steadily sought to engage other governments and organizations around the world, these efforts fall far short of what might have been achieved, had they been adequately resourced and prioritized. International engagement is crucial for ensuring a stable global system and for setting expectations for how adversaries and allies should behave in cyberspace. Building cybersecurity capacity around the globe is likewise critical if those expectations are to be enforced consistently and reliably. The United States can bolster those expectations by strengthening the coalition of democracies that stand with us and by assembling a coalition of allies and like-minded partners to collectively incentivize responsible state behavior in cyberspace, impose substantial costs on those responsible for malicious attacks, and mobilize global action on global cyber threats.

A. Establish the Bureau of Cyberspace Policy and Emerging Technologies

In order to adequately prioritize cybersecurity as an international policy issue, ***the Biden-Harris administration should establish the Bureau of Cyberspace Policy and Emerging Technologies (CPET) at the State Department.*** CPET should be designed and equipped to lead in forming an international coalition and be responsible for implementing aspects of the United States' broader cybersecurity strategy. Mirroring the structure and responsibilities outlined in the proposed Cyber Diplomacy Act of 2019,[8] this bureau must have the authority to lead across a wide range of issues, including advocating for norms of responsible state behavior in cyberspace, reinforcing confidence-building measures, responding diplomatically with the international community to cyber threats, promoting an open and interoperable internet governed by the multi-stakeholder model, ensuring international collaboration to achieve a secure digital economy, building capacity in our partners and allies to promote cybersecurity and combat cybercrime, and undertaking any other mission areas that the Secretary of State assigns to it.

B. Expand U.S. Government Support for Capacity Building, Norms, and Confidence-Building Measures

With CPET in place, ***the Biden-Harris administration should leverage the bureau to expand U.S. government support for capacity building, diplomacy around norms, and cyber confidence-building measures (CBMs).*** In several forums, including the United Nations, the international community has agreed to cyber norms. However, these norms have been unevenly implemented and enforced. The U.S. government, led by CPET, should take a multi-stakeholder, sector-by-sector approach to norms implementation,[9] lead discussions about cybersecurity norms at the head-of-state level, and engage in both inclusive and exclusive forums at the United Nations and elsewhere. The administration should work with Congress to ensure that CPET has the personnel, resources, and authorities needed to incentivize and enable responsible state behavior in cyberspace through capacity-building efforts. Furthermore, the Department of State should continue to develop and implement both regional and global cyber CBMs, engaging as well with non-state stakeholders such as private-sector entities. The administration should also ensure that international cybersecurity capacity-building efforts reflect the integral role played by these activities in U.S. foreign policy. Through the establishment of international partnerships and coalitions, capacity building—and international engagement more broadly—is a critical step toward restoring American leadership.

C. Engage More Actively and Effectively in International ICT Standards Forums

In addition to expending more effort on norms and CBMs, the U.S. government must engage more actively and effectively in international ICT standards-setting forums. To do so, ***the Biden-Harris administration should work with Congress to ensure that federal departments and agencies have the resources and authorities they need to facilitate robust and integrated U.S. participation by individuals from the federal government, academia, professional societies, and industry in forums setting ICT standards.*** To participate more effectively, the U.S. government should proactively engage with stakeholders across sectors prior to and simultaneous with discussions on ICT standards. Furthermore, leaders in the executive branch should send not only technical and standards experts but also diplomats to participate in ICT standards forums.

2. INVEST MORE IN THE PEOPLE WE NEED TO DEFEND AGAINST MALICIOUS CYBERATTACKS

At present, the public sector needs to fill more than 37,000 cybersecurity jobs. Given that the sector currently employs more than 56,000 cybersecurity professionals, this shortfall means that about one in three public-sector cybersecurity jobs sits unfilled. Meanwhile firms are confronted with the challenge of filling almost half a million cybersecurity jobs.[10] To address unfilled federal cyber jobs in 2009, experts called for the White House cybersecurity coordinator to develop a federal cyber workforce strategy.[11] Twelve years later, the U.S. federal government still does not have an effective cyber workforce strategy or any clear leader responsible for developing and implementing such a strategy.

A. Establish Workforce Leadership and Coordination Structures

Across the U.S. government, many departments and agencies are taking steps to grow their cyber workforce; however, there is no central leadership or strategy to coordinate these efforts. To fill this function, ***the Biden-Harris administration should establish two bodies on federal cyber workforce development and work with these bodies to draft a federal cyber workforce strategy.*** First, the administration should establish a Cyber Workforce Steering Committee (CW-SC) chaired by the National Cyber Director and consisting of representatives from the Office of Management and Budget, the Office of Personnel Management (OPM), the National Initiative for Cybersecurity Education, the National Science Foundation, CISA, and the Department of Defense (DoD). The CW-SC should provide leadership-level strategic guidance and direct resources to ensure a coordinated approach to cyber workforce development across the federal government. Meanwhile, a Cyber Workforce Coordinating Working Group, open to all departments and agencies, should address the day-to-day development and operation of programs and ensure that they are chartered, resourced, and aligned with the strategic direction

established by the Steering Committee. Working with these two bodies—as well as with federal departments and agencies not listed above, like the Department of Education, that also play important roles in scaling cyber workforce development efforts nationwide—the National Cyber Director should develop a cyber workforce strategy that limits duplication of effort, ensures strategically beneficial distribution of resources, and reduces interagency competition for the same talent pools. By establishing these bodies and instituting a workforce strategy, the National Cyber Director can serve as a central voice advocating for effective, integrated workforce development.

B. Ensure Availability of Special Hiring Authorities and Pay Flexibilities for Cyber across the U.S. Government

The ability to use special hiring authorities and pay flexibilities for cyber talent is distributed unevenly across the federal government. Many departments and agencies struggle to decipher and use a complex system of occupational coding and authorities, while others have bypassed this route entirely in favor of developing department-specific personnel management systems. In order to foster the flexibility and innovation needed to build the future federal cyber workforce, ***the Biden-Harris administration should work to eliminate existing barriers to using special hiring authorities and pay flexibilities across the whole of the federal government.*** In reports issued in 2018 and 2019, the Government Accountability Office outlined challenges to classifying federal cyber jobs, which limited the use of hiring authorities and pay flexibilities.[12] Subsequently, OPM provided information to assist federal managers in implementing the tools. The incoming administration should evaluate whether OPM's efforts have been sufficient to make the existing system effective for managing cyber talent. If not, the administration should direct OPM to develop multiple occupational series designations specific to cyber to enable greater use of special hiring authorities and pay flexibilities.

C. Expand the CyberCorps Scholarship for Service Program

The CyberCorps Scholarship for Service (SFS) program was structured to be cost-effective and scalable by building on the educational infrastructure of existing colleges and universities, but in recent years a stagnant budget has prevented SFS from maximizing its potential. ***The Biden-Harris administration should prioritize the requirements of Scholarship for Service in budgetary requests to Congress in order to (1) increase the number of colleges and universities that participate in the program and (2) increase the number of scholarships awarded at participating institutions.*** Practical constraints dictate that this expansion must happen gradually, at an average annual rate of 20 to 30 percent above inflation over a 10-year period. This would bring the program's budget to $80 million for fiscal year 2022. To the extent possible, the program should particularly strive to encourage participation from minority-serving institutions as a means of promoting much-needed diversity in the cyber workforce.

3. INVEST IN THE RESILIENCY OF OUR INFRASTRUCTURE

The majority of assets, functions, and entities in the cyber domain that are attractive targets for adversaries are owned and operated by the private sector; as a result, cyber defense, while a shared responsibility, depends significantly on the underlying efforts of the owners and operators of private networks and infrastructure.

A. Begin Continuity of the Economy Planning

The FY2021 NDAA requires the President to "develop and maintain a plan to maintain and restore the economy of the United States in response to a significant event."[13] ***The Biden-Harris administration should begin the process of developing a Continuity of the Economy plan.*** While the U.S. government maintains Continuity of Operations and Continuity of Government plans, no equivalent exists to ensure the continuity of the economy, a critical source of American national power. The planning process should include the Department of Homeland Security, Department of Defense, Department

of Commerce, Department of the Treasury, Department of Energy, Department of Health and Human Services, the Small Business Administration, and any other departments or agencies as determined by the President.

As part of the planning process, the executive branch should determine any additional authorities or resources that would be required to implement plans should a disaster occur or to establish programs that support and maintain department and agency planning capabilities for Continuity of the Economy efforts. The planning process should analyze National Critical Functions,[14] focusing on the national-level distribution of goods and services necessary for the reliable economic functioning of the United States; it should also outline the key private-sector entities that constitute or are integral to these distribution mechanisms and bear primary responsibility in maintaining and operating them for specific sectors or regions or for the economy as a whole. In addition, the plan should identify key materials, goods, and services; response and recovery priorities; areas for resilience investment; and areas where data must be preserved.

B. Explore the Viability of Sharing Information at Machine Speed

The Biden-Harris administration should task the Secretary of Homeland Security and the Director of National Intelligence with drafting a report on the feasibility and advisability of establishing a joint, cloud-based information-sharing environment in which the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made generally available for query and analysis.

C. Improve Intelligence Support to the Private Sector

While the intelligence community is formidable in informing security operations in instances when the U.S. government is the defender, it lacks appropriate policies and processes to deal with instances when primary responsibility falls outside of the U.S. government. Intelligence policies and procedures have not been updated to take into account that unique information gathered by the U.S. intelligence community is essential to the defense of digital infrastructure owned and operated by the private sector, or that malicious foreign actors have become more flexible and ingenious. As a result, the intelligence community continues to be significantly limited in its ability to maintain awareness of evolving cyber threats and provide essential warning to U.S. entities when they are being targeted. The U.S. government must address more general limitations in its ability to provide intelligence support to all private-sector stakeholders and associated organizations, such as information sharing and analysis centers and the Analysis and Resilience Center for Systemic Risk.

To that end, ***the Biden-Harris administration should conduct a six-month comprehensive review of intelligence policies, procedures, and resources to identify and address key limitations in the ability of the intelligence community to provide intelligence support to the private sector.*** The executive branch should report its findings to Congress upon conclusion of this review, which should include specific recommendations or plans to address challenges identified in the report. The review should examine intelligence authorities to identify existing limitations in collection for supporting private-sector stakeholders, review limitations on the intelligence community's ability to share intelligence with private-sector stakeholders, review the procedures for downgrading and declassifying cyber threat intelligence, and review cyber-related information-sharing consent processes. ***In addition, the Biden-Harris administration should establish a formal process to solicit and compile private-sector input to inform national intelligence priorities, intelligence collection requirements, and more focused U.S. intelligence support to private-sector cybersecurity operations.***

4. SAFEGUARD AMERICA'S HIGH-TECH SUPPLY CHAINS

As the Commission noted in its October 2020 white paper, where ICT supply chains are concerned, "the United States has a China problem."[15] Because of Chinese state intervention, the international system of commerce in critical technologies is neither free nor fair, hampering the ability of American and partner companies to compete for global market share and be

part of a secure and reliable supply chain. However, as the SolarWinds incident has underscored, while China poses a major risk to the United States' supply chains, the threats do not stop at the Chinese border. The United States must do more to identify risks in our ICT supply chains and devote resources to managing them.

A. Develop and Promulgate an ICT Industrial Base Strategy

While the FY2021 NDAA sets in motion several initiatives to help the United States understand the scope of the problem, unlock some public investment vehicles, and engage more robustly in crucial standards-setting forums, the United States still lacks a comprehensive overarching strategy to secure America's ICT supply chains by ensuring that the rules of the road benefit our workers and our economy, as well as by helping our companies and those in partner and ally countries compete globally in the face of anti-competitive Chinese state interventions in markets. ***The Biden-Harris administration should develop and promulgate an industrial strategy to safeguard America's high-tech future.*** The strategy should be built on a firm foundation of partnership—with American industry, allied governments, and foreign companies in allied and partner nations—and should rest on five distinct pillars. The strategy should

1. ***Identify key technologies, equipment, and raw materials*** through a government review and through consultation with industry.[16]

2. ***Ensure minimum viable manufacturing capability in essential areas*** by aligning private investment with critical manufacturing needs, providing government investment where absolutely necessary, and aiding economic clusters through a mix of investment and economic protections.

3. ***Protect supply chains from compromise*** through better coordination at the federal government level, enhanced intelligence support to the private sector, and more robust vulnerability testing for critical technologies.

4. ***Stimulate a domestic market for ICTs*** by releasing more mid-band spectrum and tying future government investment in ICTs to open and interoperable standards.

5. ***Enable global competitiveness of American and partner companies*** by strategically leveraging existing tools at the Export-Import Bank of the United States, the U.S. International Development Finance Corporation, the U.S. Trade Development Agency, and the U.S. Agency for International Development.

5. PRESERVE AMERICA'S MILITARY CYBER ADVANTAGE

The United States possesses one of the most mature and advanced military-cyber capabilities in the world. However, unless attention, assessment, and investment increase, this military-cyber advantage may atrophy or disappear. Many of the recommendations below appear in the FY2021 NDAA but require attention and implementation from the executive branch.

A. Conduct a Force Structure Assessment of the Cyber Mission Force

The Cyber Mission Force (CMF) is currently considered to be at full operational capability, with 133 teams comprising a total of approximately 6,200 individuals. But these requirements were defined in 2013, well before some of the key events that have shaped the U.S. government's understanding of the urgency and salience of the cyber threat posed by adversaries, as well as before the development of DoD's defend forward strategy. Today, the teams that make up the CMF are responsible for a range of distinct DoD cyber missions, which include defending the DoD information network (DoDIN), providing support to military operations through the geographic combatant commands, and defending the nation to counter malicious adversary behavior in day-to-day competition. These activities represent an expansion of the scope of the CMF's

mission set (operating off DoDIN) and the scale of its operations (increasing operations in response to a more dangerous threat environment), even though its force structure goal has remained constant. ***The Biden-Harris Department of Defense should conduct a force structure assessment of the U.S. Cyber Command's Cyber Mission Force to reflect the growing scope and scale of its mission requirements and expectations.***

B. Create Major Force Program for Cyber Command

The Biden-Harris Department of Defense should submit a budget justification display that includes a major force program (MFP) category for the training, manning, and equipping of U.S. Cyber Command. According to 10 U.S. Code § 238, DoD is required to submit to Congress a budget justification display that includes an MFP category for the Cyber Mission Force. However, this law was enacted in 2014, before U.S. Cyber Command was elevated to a unified combatant command. Therefore, a new budget justification display is needed that establishes an MFP category for U.S. Cyber Command. This funding category would provide U.S. Cyber Command with acquisition authorities over goods and services unique to the command's needs. It should also provide a process to expeditiously resolve combatant command/Service funding disputes, consistent with the intent of DoD Directive 5100.03.[17] While the FY2021 NDAA does contain some improved elements—most notably the call for recommendations to enable Cyber Command to execute budget and acquisition requirements in excess of existing limits and the elimination of the $75 million annual spending cap—it does not create a major force program category for Cyber Command.[18]

C. Update the Rules of Engagement and Guidance for the Use of Force for Cyber

The Standing Rules of Engagement (SROE) and Standing Rules for Use of Force (SRUF) are more than a decade old. ***The Biden-Harris Department of Defense, as part of the next Cyber Posture Review, should produce a study that assesses the Standing Rules of Engagement and Standing Rules for Use of Force for U.S. forces and provides recommendations for amendments as necessary.*** This study should be context-specific, taking into account the forces' assigned mission sets. Given the unique aspects of operating in cyberspace, particularly below a use-of-force threshold, it is imperative that SROE/SRUF guidance be relevant to actions in and through cyberspace.

D. Assess the Establishment of a Military Cyber Reserve

The FY2021 NDAA mandates that the executive branch conduct a review of the need to establish a military cyber reserve.[19] ***The Biden-Harris Department of Defense should assess the need for, and requirements of, a military cyber reserve, its possible composition, and its structure (i.e., a retainer model, a nontraditional reserve, a strategic technological reserve, or some other model).*** This assessment of a military cyber reserve should explore how different types of reserve models could address broader issues of talent management and should consider how a cyber reserve could deliberately recruit key private-sector participants. In addition, the assessment should examine ways to effectively recruit and retain civilian talent with no prior military expertise who are interested in serving; at the same time, it should evaluate a cyber reserve's possible impact in drawing civilian talent from the private sector and from the government's non-DoD workforce. Finally, the assessment should address how DoD might use existing mechanisms to bring in technical expertise when needed to respond to a crisis and should identify shortcomings in cyber expertise that might be addressed through more targeted hiring practices.

E. Review the Defend Forward Concept and the Delegation of Authorities for Offensive Cyber Operations

The Department of Defense has continued to steadily improve its offensive cyber capabilities. In its 2018 Defense Cyber Strategy, DoD articulated a "defend forward" strategy to disrupt or degrade malicious cyber activity at its source.[20] This proactive approach has improved America's position in the cyber battlespace by leveraging the U.S. Cyber Command's "persistent engagement" concept.[21] The new strategy also draws support from three critical provisions of the FY19 NDAA

that authorized the framework for existing offensive cyber operations. Section 1632 authorized DoD to conduct cyber surveillance and reconnaissance as a traditional military activity; section 1636 established U.S. policy for responding to cyberattacks and other malicious cyber activities conducted by foreign powers; and section 1642 authorized DoD to act in response to malicious Russian, Chinese, North Korean, or Iranian cyber campaigns. The executive branch then developed National Security Presidential Memorandum 13, which authorized offensive cyber operations.[22] Despite the mandate to operate on non-U.S. networks, defend forward—as the name suggests—is a defense-oriented strategy, seeking to neutralize imminent threats before attacks are launched. These efforts remain one of the bright spots of the Trump administration's cyber policy, but ***the Biden-Harris administration should review and refine the defend forward concept and the delegation of authorities for offensive cyber operations, ensuring that the process adequately assesses risk and benefits while maintaining the required focus on swift action.***

6. PROTECT AMERICA'S FULL SPECTRUM WAR FIGHTING AND DETERRENCE CAPABILITIES FROM CYBER THREATS

America's full-spectrum war fighting and deterrence capabilities are crucial to our continued national security and form a solid foundation upon which cyber deterrence rests. Should these capabilities fail, layered cyber deterrence crumbles. It is therefore imperative that the United States protect these capabilities from cyber threats. All of the recommendations below appear in the FY2021 NDAA but require immediate attention and implementation from the executive branch.

A. Develop a Plan for Defending Nuclear Command, Control, and Communications from Cyberattacks

The United States' nuclear capability is the cornerstone of our overarching deterrence posture. Without an operational nuclear capability, all aspects of our ability to deter adversary action—including cyberattacks—fail. To ensure the continuous function of our nuclear weapons systems and diminish their vulnerability, ***the Biden-Harris administration should implement the FY2021 National Defense Authorization Act mandate to develop a concept of operations for defending the nuclear command, control, and communications system against cyberattacks.***

B. Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program

The FY2021 NDAA mandates a report from the Secretary of Defense on the feasibility and suitability of a program requiring that threat intelligence be shared within the Defense Industrial Base (DIB) and between the DIB and the Department of Defense.[23] This is a good start, but ***the Biden-Harris administration should go beyond a report and pass a policy directive requiring companies that make up the Defense Industrial Base, as part of the terms of their contract with DoD, to participate in a threat intelligence sharing program that would be housed at the DoD component level.***

C. Require Threat Hunting on Defense Industrial Base Networks

The FY2021 NDAA mandates a report from the Secretary of Defense on the feasibility and suitability of a program requiring threat hunting on DIB networks.[24] ***The Biden-Harris administration should go beyond a report and pass a policy directive requiring companies that make up the Defense Industrial Base, as part of the terms of their contract with DoD, to create a mechanism that allows mandatory threat hunting on DIB networks.***

A POSITIVE CYBER LEGISLATIVE AGENDA FOR THE BIDEN-HARRIS ADMINISTRATION

By drawing on existing authorities and appropriations, the executive branch can make great progress in rebuilding America's cybersecurity, but some CSC recommendations cannot be implemented without congressional support and approval. The Biden-Harris administration should work with Congress to ensure that the United States is best positioned to prevent, withstand, respond to, and ultimately recover from significant cyber incidents. A positive cybersecurity legislative agenda for the administration should focus on building better cyber expertise in government, institutionalizing international cyber engagement, promoting a more secure national cyber ecosystem, investing in cyber resiliency, creating support for victims of cyber crime, and protecting American democracy.

1. BUILD BETTER CYBER EXPERTISE IN GOVERNMENT

Both the executive and legislative branches of the federal government would benefit from greater cyber policy expertise and more robust metrics and data to help drive cyber policy. The Biden-Harris administration should work with Congress to implement two recommendations from the CSC final report that are aimed at building this capacity: (1) establishing a Bureau of Cyber Statistics within the executive branch and (2) codifying and strengthening the Cyber Threat Intelligence Integration Center.

A. Establish the Bureau of Cyber Statistics

While there is broad consensus that cyberattacks on U.S. citizens and businesses are increasing in frequency and severity, the U.S. government and broader marketplace need more information about the nature and scope of these attacks so that they can develop nuanced and effective responses. To address similar gaps in other policy areas, the United States established statistical agencies, such as the Bureau of Economic Analysis, the Bureau of Labor Statistics, and the Census Bureau, to inform both public policymaking and private decision making. ***The Biden-Harris administration should work with Congress to establish a Bureau of Cyber Statistics within the Department of Commerce***, or another department or agency, that would act as the government agency that collects, processes, analyzes, and disseminates essential statistics on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other federal agencies, state and local governments, and the private sector.

B. Codify and Strengthen the Cyber Threat Intelligence Integration Center

The Cyber Threat Intelligence Integration Center (CTIIC) plays a critical role in generating a whole-of-government understanding of significant cyber threats affecting the United States and could assist in providing the analysis and coordination necessary for rapid and accurate attribution. However, to carry out the entire scope of its mission CTIIC needs to be fully resourced, including sufficient funding, manpower, and analytical resources to fully support federal departments and agencies in carrying out their operations and in providing intelligence products to private-sector and international partners. ***The Biden-Harris administration should work with Congress to codify and establish the Cyber Threat Intelligence Integration Center through legislation and to ensure its adequate resourcing.***

2. INSTITUTIONALIZE INTERNATIONAL CYBER ENGAGEMENT

While the Biden-Harris administration can take some steps to reprioritize international cyber engagement through the Department of State, to meaningfully elevate and institutionalize international cyber engagement it must create a new bureau and an associated Ambassador-at-Large for Cyberspace Policy and Emerging Technology with rank equivalent to Assistant Secretary. In the same vein, Part II of the Foreign Assistance Act of 1961 should be changed to provide more effective structural support to critical cybersecurity capacity-building programs worldwide.

A. Codify a Bureau for Cyberspace Policy at the State Department

The Biden-Harris administration should work with Congress to codify in law a State Department bureau dedicated to cyberspace policy and led by an Ambassador-at-Large for Cyberspace Policy with rank equivalent to Assistant Secretary reporting to the Under Secretary for Political Affairs or official of higher rank. The proposed Cyber Diplomacy Act of 2019 provides a basis for this future legislation. In addition to guiding the formation of a coalition of like-minded partners and allies, the bureau should be responsible for a range of mission sets, including advocating for norms of responsible state behavior in cyberspace and confidence-building measures, responding diplomatically with the international community to cyber threats, advocating for internet freedom, ensuring a secure digital economy, building capacity in our partners and allies to promote cybersecurity and combat cybercrime, and undertaking any other mission areas that the Secretary of State assigns to it. The administration should work with Congress to provide additional funding to this new bureau for its personnel and programs needed to carry out its international cyber mission, especially the mission of building a robust coalition.

B. Maximize Flexibility in International Cybersecurity Capacity Building

Cybersecurity capacity building incentivizes responsible state behavior by providing resources and expertise to states that abide by established norms. Moreover, it provides a practical pathway for like-minded foreign governments to help their national cybersecurity enterprise become more mature. For states that want to curtail cybercrime and other malicious activities emanating from within their borders but lack the means to do so, the provision of this support improves cybersecurity globally. While the U.S. government engages in cyber capacity building through a broad range of mechanisms, one of the primary resources—the Economic Support Fund—can be used to support only activities that are not "military or paramilitary." However, because many foreign governments house their civilian public-sector cybersecurity infrastructure within such agencies, this restriction prevents support from reaching actors critical to civilian cybersecurity. Accordingly, ***the Biden-Harris administration should work with Congress to authorize the use of funds appropriated for projects designed to strengthen foreign countries' civilian cybersecurity without limitations imposed because recipients' cybersecurity agencies are housed within particular agencies.***

3. PROMOTE A MORE SECURE NATIONAL CYBER ECOSYSTEM

Today, the cyber ecosystem is more than the technology—information, network, and operational technology—that constitutes the internet. It is also the people, processes, and organizations that plug into the technology and the data that they combine to produce. This ecosystem has increased the speed of our communications, as well as efficiency, functionality, and growth in the economy. But though this ecosystem is central to the functioning of the nation, it has also introduced significant challenges and opened up potential harms across the United States. Adversaries leverage its vulnerabilities and its expansive reach into our society to gain an asymmetric advantage, developing capabilities to hold our critical infrastructure at risk, disrupt our elections, and spy on and target the data, systems, and resilience of the American people. The Biden-Harris administration should take steps to lessen vulnerability across the ecosystem by shifting the burden of security away from end users to owners and operators, developers, and manufacturers who can more effectively implement security solutions at the appropriate scale.

A. Create a National Cybersecurity Certification and Labeling Authority

While agreed-on security standards and best practices are useful in reducing vulnerability in information technology products, they can be employed more effectively if product developers come to treat security as a product differentiator. Without accessible and transparent mechanisms, such as certifications and labels, that enable purchasers to compare products' level of security, critical infrastructure owners and operators cannot easily price security into their purchasing decisions. ***The Biden-Harris administration should work with Congress to pass legislation granting the Department of Commerce, in coordination with the Department of Homeland Security and the Department of Defense, the funding and authorities to hold a competitive bid for a nonprofit, nongovernmental organization to be designated and funded as the National Cybersecurity Certification and Labeling Authority.***

B. Pass an Internet of Things Security Law

With a significant portion of the workforce working from home during the COVID-19 pandemic, household internet of things (IoT) devices, particularly household routers, have become important but vulnerable pieces of our national cyber ecosystem and our adversary's attack surface.[25] The 116th Congress passed the IoT Cybersecurity Improvement Act of 2020, which represents an important first step in improving the security of the United States' IoT ecosystem by mandating baseline security requirements for IoT devices purchased by the federal government.[26] ***The Biden-Harris administration should work with Congress to pass an internet of things security law to ensure that the manufacturers of IoT devices build basic security measures into the products they sell in the U.S. market.*** The law should focus on known challenges, like insecurity in Wi-Fi routers, and mandate that these devices have reasonable security measures, such as those recently outlined by the National Institute of Standards and Technology as "foundational cybersecurity activities recommendations for IoT device manufacturers."[27]

C. Create an IT Modernization Grant Program for State, Local, Tribal, and Territorial Governments

The pandemic has produced new realities that demonstrate the importance of digitizing critical services. During the outbreak, Americans have increasingly relied on federal and state aid programs whose legacy systems have been stressed to the brink of failure. To survive future pandemics or catastrophic cyber incidents, the nation needs secure, remote access to reliable digital services. Modernization and digitization, though expensive in the short term, create greater efficiency and flexibility in the delivery of services while reducing spending, increasing productivity, and shrinking the economic disparity between digital haves and have-nots in the long term. Nonetheless, state, local, tribal, and territorial governments and small businesses regularly defer digitization in pursuit of shorter-term funding priorities. This short-term trade-off produces damaging long-term consequences. America is now paying the price for decades of short-term thinking. Consistent with the Biden-Harris administration's intent to invest in America's physical infrastructure, ***the Biden-Harris administration should work with Congress to include grants to state, local, tribal, and territorial governments in future COVID-19 stimulus legislation so that these entities can more quickly move to the cloud and modernize their digital infrastructure.*** The proposed State and Local IT Modernization Cybersecurity Act provides a basis for future legislation.[28]

D. Clarify the Legal Liability of Final Goods Assemblers of Hardware, Software, and Firmware

Software vulnerabilities present cracks in systems that our adversaries seek to exploit. Shortening the lifecycle of vulnerabilities by ensuring that patches are created and implemented in a timely manner would limit their availability to those who seek to exploit them, driving up adversaries' operating costs and denying them the benefits that successful exploitation could bring.[29] To encourage final goods assemblers of hardware, software, and firmware to shorten the vulnerability lifecycle by more quickly developing and issuing patches, ***the Biden-Harris administration should work with Congress to institute a duty of care in law, establishing that final goods assemblers of software, hardware, and firmware are liable for damages***

from incidents that exploit vulnerabilities that were known at the time of shipment or were discovered and not fixed within a reasonable amount of time.

E. Pass a National Data Breach Notification Law

Data breach notification laws require an entity that has been the victim of a data breach—regardless of cause—to notify its customers and other relevant parties and to take steps to remediate injuries caused by the breach. While such laws have been adopted in some form by all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, there is no national standard for such notification.[30] As a result, Americans' data is subject to a patchwork of varying protections. A national framework is needed to standardize consumers' expectations and provide regulatory certainty to American businesses engaging in interstate and global commerce. ***The Biden-Harris administration should work with Congress to pass a national data breach notification law that standardizes data breach notification requirements in the United States and preempts the 54 existing state, district, and territorial data breach notification laws.***

4. INVEST IN CYBER RESILIENCY

The U.S. government should increase its support of private-sector cyber defensive operations. Given its limited resources and capabilities, however, the federal government should prioritize the defense of systemically important critical infrastructure—the critical infrastructure entities that manage systems and assets whose disruption could have cascading, destabilizing effects on U.S. national security, economic security, or public health and safety.

A. Codify Systemically Important Critical Infrastructure in Law

Through Section 9 of Executive Order 13636, the Obama administration took vital steps to recognize that not all critical infrastructure is equally important to the preservation of public health and safety, economic security, or national security.[31] But that effort falls short of codifying or fully implementing the social contract of shared responsibility and partnership in cybersecurity that the order acknowledges. Moreover, Section 9 does not endow the U.S. government with any new requirements, resources, or authorities to support systemically important critical infrastructure; nor does Section 9 designation place any additional expectations on the entities that receive it. ***The Biden-Harris administration should work with Congress to build on Executive Order 13636 by passing a bill that codifies in law the concept of "systemically important critical infrastructure."*** The law should ensure that entities responsible for systemically critical systems and assets are granted special assistance from the U.S. government and are responsible for shouldering the additional security and information-sharing requirements that befit their unique status and importance.

B. Establish a National Risk Management Cycle

The Biden-Harris administration should work with Congress to pass a bill that establishes a national risk management cycle and a national critical infrastructure resilience strategy to coordinate and streamline national risk management efforts. This cycle should be led by the Department of Homeland Security but incorporate all SRMAs; after defining procedures for identifying, assessing, and prioritizing risks, it should translate this understanding into strategy, budget, and programmatic priorities for relevant departments and agencies. These processes and procedures should be developed in consultation with critical infrastructure owners and operators, be posted publicly and made available for public comment, and be adaptive and iterative to account for lessons learned from previous cycles. Risk identification and assessments formed in the cycle should directly inform and culminate in a Critical Infrastructure Resilience Strategy, which will set programmatic and budgetary priorities for SRMAs to be implemented in the following five-year National Risk Management Cycle.

5. CREATE SUPPORT FOR VICTIMS OF CYBERCRIME

The uptick in fraud and other malicious activity during the COVID-19 pandemic has provided an unwelcome reminder that major emergencies present opportunities for criminals to further stress overburdened public services and the American people. ***The Biden-Harris administration should work with Congress to create institutions that would provide relevant support to victims of cybercrime by creating a National Cybercrime Victim Assistance and Recovery Center, as well as a grants program to fund nonprofits that aid victims of cyber crime.***

6. PROTECT AMERICAN DEMOCRACY

The U.S. government should ensure the security of our elections and resilience of our democracy. Americans' trust and confidence in their democratic system remain foundational elements of national resilience—and an attractive target for malicious actors. The network of institutions, tools, and personnel that compose our electoral system depend on connectivity and data, introducing new vectors to disrupt the U.S. political system, including at and beyond the ballot box. The federal institutions charged with protecting our electoral process require organizational reform, enduring funding streams, and modern mandates to ensure that states and other partners in our political system, including political parties and campaigns, can improve and maintain their cybersecurity capacity. In addition, Americans must become better equipped to recognize cyber-enabled information operations, so that the damage they wreak can be minimized. These information operations endanger our national security by threatening to undermine trust and confidence in American democracy and its institutions—including but also extending beyond our elections.

A. Enhance and Improve the Structure of the Election Assistance Commission

The federal institutions charged with protecting our electoral process, including the Election Assistance Commission, require organizational reform, enduring funding streams, and modern mandates to ensure that states and other partners in our political system can improve and maintain their cybersecurity capacity. ***The Biden-Harris administration should work with Congress to strengthen the ability of the Election Assistance Commission to protect American democracy.***

B. Promote Digital Literacy, Civics Education, and Public Awareness

Democracy is also threatened by adversary information operations, often cyber-enabled, that are designed to undermine public trust in democratic institutions. The pernicious narratives spread by these operations target the very notion of truth, convey an image of a system that is irrevocably broken, and exacerbate deep divisions. The process of building public resilience against this messaging starts with a renewed focus on civic education to remind Americans what democracy is about—that it is not inevitable but must be fought for, that it is worth fighting for not because it is perfect but because it is capable of positive change, and that each of us must be effective agents of that change through lawful means. ***The Biden-Harris administration should work with Congress to provide support for reinvigorating digital literacy and civics education across our nation.***

ABBREVIATIONS

CBM	confidence-building measure
CISA	Cybersecurity and Infrastructure Security Agency
CMF	Cyber Mission Force
CPET	Bureau of Cyberspace Policy and Emerging Technologies
CSC	U.S. Cyberspace Solarium Commission
CTIIC	Cyber Threat Intelligence Integration Center
CW-SC	Cyber Workforce Steering Committee
DIB	Defense Industrial Base
DoD	Department of Defense
DoDIN	Department of Defense information network
FY	fiscal year
ICT	information and communications technology
IT	information technology
IOT	Internet of Things
JCPO	Joint Cyber Planning Office
MFP	major force program
NDAA	National Defense Authorization Act
OPM	Office of Personnel Management
SFS	Scholarship for Service
SRMA	Sector Risk Management Agency
SROE	Standing Rules of Engagement
SRUF	Standing Rules for Use of Force

ENDNOTES

1 David Alexander, "Hagel, Ahead of China Trip, Urges Military Restraint in Cyberspace," *Reuters*, March 28, 2014, https://www.reuters.com/article/us-usa-defense-cybersecurity/hagel-ahead-of-china-trip-urges-military-restraint-in-cyberspace-idUSBREA2R1ZH20140328.

2 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 [FY2019 NDAA], § 1652, 132 Stat. 2141 (2018), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.

3 These publications are available at the Cyberspace Solarium Commission's website, www.solarium.gov.

4 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 [FY2021 NDAA], § 1752 (2021), available as enrolled bill at https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr.

5 FY2021 NDAA, § 9002.

6 FY2021 NDAA, § 1715.

7 U.S. Congress, Joint Explanatory Statement, "Division F — Department of Homeland Security Appropriations Act, 2021" (to Accompany the Consolidated Appropriations Act, 2021), 116th Cong., 2d sess. (2020), 51, https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-F.pdf.

8 Cyber Diplomacy Act of 2019, H.R.739, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/739/text.

9 For a leading example of a sector-by-sector approach, see Tim Maurer and Arthur Nelson, *International Strategy to Better Protect the Financial System Against Cyber Threats* (Washington, DC: Carnegie Endowment for International Peace, 2020), https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf.

10 "Cybersecurity Supply/Demand Heat Map," CyberSeek, accessed December 10, 2020, https://www.cyberseek.org/heatmap.html.

11 "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce" (Partnership for Public Service and Booz Allen Hamilton, July 2009), 19, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security__Strengthening_the_Federal_Cybersecurity_Workforce-2009.07.22.pdf.

12 "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (U.S. Government Accountability Office, June 2018), https://www.gao.gov/assets/700/692498.pdf; "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" (U.S. Government Accountability Office, March 2019), https://www.gao.gov/assets/700/697462.pdf.

13 FY2021 NDAA, § 9603.

14 "National Critical Functions," Cybersecurity & Infrastructure Security Agency, accessed January 14, 2021, https://www.cisa.gov/national-critical-functions.

15 Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain," CSC White Paper #4 (October 2020), ii, available at https://www.solarium.gov/public-communications/supply-chain-white-paper.

16 The work undertaken by the National Telecommunications and Infrastructure Agency to generate a software bill of materials (SBOM) provides a good example of a program that offers a framework to effectively understand key interdependencies and identify foundational or core components and technologies.

17 U.S. Department of Defense Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands" (February 9, 2011; incorporating Change 1, September 7, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510003p.pdf.

18 FY2021 NDAA, § 1746, 1711.

19 FY2021 NDAA, § 1730.

20 U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy 2018" (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

21 Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

22 Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

23 FY2021 NDAA, § 1737.

24 FY2021 NDAA, § 1739.

25 Allan Liska, "Remote Threats to Remote Employees: How Working from Home Increases the Attack Surface," Recorded Future, March 26, 2020, https://www.recordedfuture.com/remote-attack-surface/; "UK and US Security Agencies Issue COVID-19 Cyber Threat Update," U.S. Cybersecurity & Infrastructure Security Agency, April 8, 2020, https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update.

26 IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1001 (2020), https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

27 Michael Fagan, Katerina N. Megas, Karen Scarfone, and Matthew Smith, "Foundational Cybersecurity Activities for IoT Device Manufacturers," NISTIR 8259, National Institute of Standards and Technology, May 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

28 State and Local IT Modernization and Cybersecurity Act, H.R. 8048, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/8048.

29 Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle" (Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2017), https://www.belfercenter.org/sites/default/files/files/publication/CounteringProliferationofMalware.pdf.

30 "2019 Security Breach Legislation," National Conference of State Legislatures, July 26, 2019, http://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx.

31 Exec. Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 C.F.R. 217 (2014), https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

COMMISSIONERS

CO-CHAIRMEN

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

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

COMMISSIONERS

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

John C. "Chris" Inglis, U.S. Naval Academy Looker Chair for Cyber Studies

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

STAFF

STAFF
Mark Montgomery
Deb Grays
Laura Bate
Erica Borghard
Tasha Jhangiani
Robert Morgus
Natalie Thompson

WHITE PAPER LEAD WRITER
Robert Morgus

SENIOR ADVISORS
Tatyana Bolton
Benjamin Jensen
Alison King
Shawn Lonergan
Brandon Valeriano

LEGAL ADVISORS
Stefan Wolfe, General Counsel
David Simon, Chief Counsel for Cybersecurity and National Security

PRODUCTION STAFF
Alice Falk, Editor
Laurel Prucha Moran, Graphic Designer


U.S. CYBERSPACE SOLARIUM COMMISSION
E PLURIBUS UNUM