Testimony of:
The Honorable Angus King,
The Honorable Mike Gallagher, and
Mr. Chris Inglis

Commissioners of the
Cyberspace Solarium Commission

Before the Subcommittee on Cybersecurity of the United States Senate Committee on Armed Services

"Review of the Recommendations of the Cyberspace Solarium Commission"

August 4, 2020

INTRODUCTION - INTENT OF THE COMMISSION AND FOCUS OF OUR EFFORT

Our American way of life depends on a global, interconnected, and interdependent cyberspace which has created the modern United States' economy and society. At the same time, cyberspace creates political and strategic opportunities for malicious actors seeking to undermine our national security, economy, and political system. For these reasons, the Cyberspace Solarium Commission was established by the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The Commission is composed of fourteen Commissioners, including four currently serving legislators, four executive branch leaders, and six recognized experts with backgrounds in industry, academia, and government service, and this composition is unique to this Commission. Led by Senator Angus King and Representative Mike Gallagher, the Commission spent the past thirteen months studying the challenges facing the United States in cyberspace, developing potential solutions, and deliberating courses of action to produce a comprehensive report. Our Commissioners convened nearly every Monday that Congress was in session for over a year, conducting a total of 30 meetings. The staff conducted more than 400 engagements with industry; federal, state, and local governments; academia; non-governmental organizations; and international partners. The Commission also recruited our nation's leading cybersecurity professionals and academic minds to rigorously stress test the findings and red team the different policy options in an effort to distill the optimal approach to securing the United States in cyberspace.

The Commission's final report was presented to the public on March 11, 2020, and identified 82 specific recommendations. These bi-partisan recommendations were then subsequently turned into 54 legislative proposals that have been shared with the appropriate Committees in the Senate and the House of Representatives. Our Commissioners have now testified before Congress five times to impress upon you the urgency of the cyber threat faced by the United States today.

In addressing the NDAA's tasking, the Commission found that our critical infrastructure—the systems, assets, and entities that underpin our national security, economic security, and public health and safety—are increasingly threatened by malicious cyber actors. Effective critical infrastructure security and resilience requires reducing the consequences of disruption, minimizing vulnerability, and disrupting adversary operations that seek to hold our assets at risk. Not only does our critical infrastructure provide the foundation for our economic and societal strength, but without functioning logistics networks, power generation and distribution, and other critical functions, our military would be debilitated. In short, resilience *is* national defense.

The Commission identified a number of DoD specific proposals, all of which were taken up by your Committee and edited and improved by your staff, these include: conducting a **force**

structure assessment of the Cyber Mission Force; **reviewing delegation of DoD authorities** to enable more rapid decision-making to conduct cyber campaigns; requiring companies within the defense industrial base (DIB) to participate in a **threat intelligence sharing program** and mandatory **threat hunting on DIB networks**, examining the establishment of a **cyber reserve force**; and, clarifying the cyber capabilities and strengthen the **interoperability of the National Guard**, all of these have been included in both the House and the Senate versions of the NDAA. In addition, several recommendations are only in the Senate version, these include: creating a **major force program funding category for the U.S. Cyber Command,** conducting a **cybersecurity vulnerability assessment** of all segments of the nuclear control system and **continual assessment of our conventional weapon systems' cyber vulnerabilities**.

While we do not want to lose sight of the responsibility that this Committee has to focus on military issues, we also recognize that our national security – particularly with respect to cyberspace – cannot rely on the Department of Defense as the only stakeholder. To that end, we urge the Committee to consider the full scope of the 82 recommendations that the Commission proposed in our full report.

The future of our national security requires both the executive branch and Congress to work in tandem to prioritize and implement the key Commission recommendations to build a more effective government cybersecurity capability. These include establishing a **National Cyber Director** in the Executive Office of the President; **strengthening the Cybersecurity and Infrastructure Security Agency** (CISA) to lead interagency coordination and coordination between the Federal government and private sector; developing a **Continuity of the Economy Plan** to ensure the public and private sectors are prepared to rapidly restart our economy after a major disruption; recruiting, developing, and retaining a **stronger Federal workforce**, planning and executing a **national-level cyber table-top exercise** on a biennial basis that involves senior leaders from the executive branch, Congress, state governments, and the private sector, as well as international partners; and fostering public-private collaboration to ensure coherence, agility and speed in the nation's response to cyber attacks.[1]

A second critical line of effort is building a more robust system for private-public collaboration, this includes recommendations such as establishing an **Integrated Cyber Center within CISA**, creating a **Joint Cyber Planning Office (JCPO)** to coordinate cybersecurity planning and readiness across the Federal government and between the public and private sectors; establishing and funding a **Joint Collaborative Environment** for sharing and fusing threat information; and establishing authority for **CISA to threat hunt on .gov** networks. These all also can work in concert to create a more resilient infrastructure, a significant improvement from what we have today.[2]

---

[1] The National Cyber Director and strengthening CISA recommendations are in both the House and Senate FY21 NDAAs; the CotE and stronger cyber workforce recommendations are only in the Senate FY21 NDAA; and the table-top exercise recommendation is only in the House FY21 NDAA.
[2]All four of these recommendations: the Integrated Cyber Center, the JCPO, the Joint Collaborative Environment, and CISA threat hunting on .gov are only included in the House FY21 NDAA.

Throughout the process of developing its recommendations, the Commission always considered Congress as its "customer." Through the NDAA, Congress tasked the Commission to investigate cyber threats that undermine American power and prosperity, to determine an appropriate strategic approach to protect the nation in cyberspace, and to identify policy and legislative solutions. As Commissioners, we are here today to share what the Commission learned, advocate for our recommendations, and work to assist you in any way we can to solve this serious and complex challenge.

THE CHALLENGE

The Commission's final report made clear that while the United States has, to date, successfully deterred strategic cyberattacks that rise to the level of an armed attack, below that threshold, there is a significant set of adversary behavior that the United States has not prevented. In the past few decades, adversaries have used cyberspace to attack American power and interests. We must be clear—if adversaries attack the U.S. in cyberspace, they will pay a price. The more connected and prosperous our society has become, the more vulnerable we are to aspiring great power rivals, rogue states, extremists, and criminals. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the private sector and the public at large.

The American public relies on critical infrastructure, roughly 85% of which—according to the Government Accountability Office—is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment facilities to hospitals—are connected and vulnerable. Securing the nation in the 21st century requires an interconnected system composed of both public and private networks that is secure from state and non-state threats. China commits rampant intellectual property theft to help its businesses close the technological gap, costing non-Chinese firms over $300 billion per year. Massive data breaches, including those suffered by Equifax, Marriott, and the Office of Personnel Management (OPM), enable Chinese spies to collect data on hundreds of millions of Americans.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In spring 2014, Russian-linked groups launched a campaign to disrupt Ukrainian elections that included attempts at altering vote tallies, disrupting election results through distributed-denial-of-service (DDoS) attacks, and smearing candidates by releasing hacked emails. They continue to spread hate and disinformation on social media to polarize free societies. But they have not stopped there. The 2017 NotPetya malware attack spread globally, temporarily shutting down major international businesses and affecting critical infrastructure. Russian groups have even been found surveilling nuclear power plants in the United States. In Ukraine in 2015 and 2016, they demonstrated the capability and willingness to disrupt power generation and distribution through a cyber operation.

Iran and North Korea attack U.S. and allied interests through cyberspace. Iranian cyber operations have targeted the energy industry, entertainment sector, and financial institutions.

There are also documented cases of Iranian APTs targeting dams in the United States with DDoS attacks. North Korea exploits global connectivity to skirt sanctions and sustain an isolated, corrupt regime. The 2017 WannaCry ransomware attacks hit over 300,000 computers in 150 countries, and temporarily disrupted a number of UK hospitals. According to United Nations estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year.

Beyond nation-states, a new class of criminal thrives in this environment. Taking advantage of widespread cyber capabilities revealed by major state intrusions, criminal groups are migrating toward a “crime-as-a-service” model in which threat groups purchase and exchange easily deployable malicious code on the dark web. In 2019, ransomware incidents grew by over 300% compared to 2018 and hit over 40 U.S. municipalities. More recently, opportunistic hackers have hijacked hospitals and healthcare systems during the COVID-19 pandemic, taking advantage of poorly protected systems when they were most vulnerable.

STRATEGIC APPROACH

The strategy put forth by the Commission, layered cyber deterrence, combines a number of traditional deterrence mechanisms and extends their use beyond the government to develop a whole-of-nation approach. It also updates and strengthens our declaratory policy for cyberattacks both above and below the level of armed attack. The United States must demonstrate its ability to impose costs while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking America in cyberspace. Since America relies on critical infrastructure that is primarily owned and operated by the private sector, the government cannot defend the nation alone.

Cyber deterrence is not nuclear deterrence. The fact is, no action will stop every hack. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly to successfully attack American interests through cyberspace. Layered cyber deterrence consists of three layers, each of which are underpinned by broad reformation of the way the U.S. government approaches cybersecurity. The outer layer consists of shaping behavior by leveraging non-military instruments of power and building partnerships. The second layer focuses on denying adversaries the benefits of attacks by building greater resilience in our critical infrastructure, networks, and systems and reshaping the overall cyber ecosystem towards greater defensibility and security. The inner layer consists of imposing costs on adversaries when they do attack us. And while each layer adds an essential dimension to the defense of the nation, they form an interlocking and mutually reinforcing set of activities that concurrently increase the difficulty, costs, and ultimately the will of aggressors who seek to attack our nation in and through cyberspace.

Layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries (e.g., denial and cost imposition) with forms of influence optimized for a connected era, such as promoting norms that encourage restraint and incentivize responsible behavior in cyberspace. Strategic discussions all too often prioritize narrow definitions of deterrence that fail

to consider how technology is changing society. In a connected world, those states that harness the power of cooperative, networked relationships gain a position of advantage and inherent leverage. The more connected a state is to others and the more resilient its infrastructure, the more powerful it becomes. This power requires secure connections and stable expectations between leading states about what is and is not acceptable behavior in cyberspace. It requires shaping adversary behavior not only by imposing costs but also by changing the ecosystem in which competition occurs.

Core to layered cyber deterrence is public-private collaboration to efficiently coordinate how the nation responds with speed and agility to emerging threats, not just on an ad hoc basis, but also in an institutionalized, practiced way. The federal government alone cannot solve the challenge of adversaries attacking the networks on which America and its allies and partners rely. It requires collaboration with state and local authorities, leading business sectors, and international partners, all within the rule of law. This strategy also outlines the planning needed to ensure the continuity of the economy and the ability of the United States to rebound in the aftermath of a major, nationwide cyberattack of significant consequence. Such planning adds depth to deterrence by assuring the American people, allies, and even our adversaries that the United States will have both the will and capability to respond to any attack on our interests.

SPECIFIC RECOMMENDATION FOR A NATIONAL CYBER DIRECTOR

For the past 20 years, commissions, initiatives, studies, and even four Presidential Administrations have been challenged to define and establish an effective national-level mechanism for coordinating cyber strategy, policy, and operations. It is imperative that the executive branch have a strong, stable, and expert-led cyber office and leader within the White House. To fill this gap, the Commission recommended the creation of a National Cyber Director. Similar to the way in which the Secretary of Defense's Principal Cyber Advisor (PCA) supports the DoD, the National Cyber Director would support the President by formulating, recommending, integrating, and implementing policies and strategies to improve the nation's ability to operate in cyberspace.

Former House Intelligence Committee Chairman, Mike Rogers, testified to the House Oversight and Reform Committee that "this is not an abstract problem. In April 2015, IT staffers at the Office of Personnel and Management (OPM) discovered that their systems were breached by hackers, ultimately linked to China, that extracted millions of sensitive SF-86 personnel security clearance forms and millions of fingerprint cards. This is not to say that had the National Cyber Director been in place that the OPM hack would not have happened—but it is to say that there would have been a person responsible for ensuring that the nation's cybersecurity posture was as strong and robust as possible, and whom Congress could hold accountable for failings and shortcomings." Establishing a **National Cyber Director** within the Executive Office of the President would consolidate accountability for harmonizing the executive branch's policies,

budgets, and responsibilities in cyberspace while implementing strategic guidance from the President and Congress.[3]

Situated within the Executive Office of the President, the Senate-confirmed National Cyber Director would be supported by the Office of the National Cyber Director and fill several important roles:

1. Act as the President's principal advisor on cybersecurity and associated emerging technology issues and lead development of a National Cyber Strategy and associated policies;
2. Ensure the implementation of the National Cyber Strategy across departments and agencies to include the effective integration of interagency efforts, and providing for the review of designated department and agency cybersecurity budgets.
3. Oversee and coordinate Federal government activities to defend against adversary cyber operations inside the United States, to include coordination with private sector and state, local, tribal, and territorial (SLTT) entities;
4. With concurrence from the National Security Advisor or the National Economic Advisor, convene and coordinate Cabinet-level or National Security Council (NSC) Principals Committee–level meetings and associated preparatory meetings.

Recommendation Development
Early in this process, Commissioners identified the need to create a leadership position but were faced with three key decision points: (1) how to address the gap in national leadership, coordination, and consistent prioritization, (2) whether to recommend Senate confirmation for the coordination and leadership position, and (3) the size, structure, and scope of authorities.

The Commission explored other options for cybersecurity structure like the creation of a new cabinet department for cyber, but ultimately decided to strengthen the existing agency (CISA), rather than the creating a new department, as the protracted development of a new department would prevent much-needed near-term progress. Like the DoD's PCA, it is imperative that the National Cyber Director get appropriate access to the right leadership, and be institutionalized to be successful. In contemplating the stature of the position, the Commission determined that it must sit within the EOP and be Senate confirmed to not only signal Congress' commitment to cyber issues, but also afford them a level of political support that bipartisan endorsement would bring, and ensure effective oversight. Senate-confirmation of EOP leadership is not without precedent. The heads of the Office of Management and Budget, the Office of the National Drug Control Policy, Office of Science and Technology Policy, and the Office of the United States Trade Representative are all Senate-confirmed. The Director's focus must be on creating and implementing national strategy, which further instilled the Commission's conviction that the National Cyber Director must sit apart from departments and agencies, both of which focus on

[3] The recommendation for the creation of a National Cyber Director was introduced as a standalone bill in the House as H.R.7331 and is also included in the House FY21 NDAA. A provision for an independent assessment of establishment of a National Cyber Director is included in the Senate FY21 NDAA bill.

the day-to-day responsibilities of their given mission set. The Office of the PCA at DoD, which the Commission also looked to for guidance, similarly has an office and staff to support their efforts to establish and oversee the implementation of DoD cyberspace policy and strategy.

Recommendation Details

Structure and Size of Office. The National Cyber Director should oversee and manage the Office of the National Cyber Director, and be assisted in their duties by two Deputy National Cyber Directors: the Deputy National Cyber Director for Strategy, Capabilities, and Budget and the Deputy National Cyber Director for Plans and Operations. To fulfill the full range of functions and responsibilities envisioned in the recommendation, the Commission recommends the Office of the National Cyber Director be staffed with approximately 75 to 100 full-time employees,[4] a size similar to that of existing, comparable EOP organizations. A mix of rotating detailees from other federal departments of agencies and direct-hire, full-time employees would comprise those employees.

Policy and Strategy Development and Coordination. The National Cyber Director should be the President's primary advisor on issues involving cyber, cybersecurity, federal information security, and associated emerging technologies, and statutorily appointed to the NSC. Akin to the structure Congress gave the PCA in DoD, the NCD-developed strategy would establish a clear vision, priorities, and objectives to advance the cybersecurity posture of the United States. As such, the National Cyber Director would be responsible for policy and strategy development relevant to these issues, including the development of a National Cyber Strategy, in coordination with other appropriate offices within the Executive Office of the President.

If implemented as envisioned, the National Cyber Director's primary responsibility for cyber and associated emerging technology-related policy and strategy development is not expected to limit or constrain the ability of other White House principals, such as the National Security Advisor, Homeland Security Advisor, or the National Economic Advisor, to address similar issues. However, as a statutory member of the National Security Council and as an Assistant to the President, the National Cyber Director would likely participate in Principal's Committee meetings with the President where these issues are under consideration. Given this reality, the Commission recommends that White House offices avail themselves of the expertise, participation, and guidance of the National Cyber Director (and staff) early and throughout their respective policymaking processes for issues within or related to the National Cyber Director's remit. This should serve to reduce uncoordinated, parallel processes that could undermine the overall aim of a unified, cohesive cyber strategy.

While the policy coordination authorities and responsibilities outlined above are sufficient to empower the National Cyber Director in developing a National Cyber Strategy and implementing its relevant policy changes, they alone would have limited effectiveness in driving

[4] While the Commission's March 2020 report recommended the Office of the National Cyber Director to be staffed by 50 persons, follow-up interviews with various experts consistently and strongly supported increasing the staff number to 75 to 100.

implementation through department and agency budgetary and programmatic priorities. Congress itself has acknowledged the need for budget authority for effective execution of programmatic leadership in the authorities it gave the DoD PCA to advise, advocate for, and identify shortfalls in DoD budgets with respect to DoD cyber planning. Additionally, the lack of any oversight authority for performance, programs, and budget would significantly limit the National Cyber Director's ability to negotiate compromises among departments and agencies, forge consensus, and drive the President's agenda, something the DoD PCA authorizing legislation (FY2014 NDAA as amended in FY2020 NDAA) addressed by providing the PCA the ability to provide recommendations on addressing such shortfalls in the Program Budget Review process. The Commission recommends that the National Cyber Director be granted, in coordination with the Office of Management and Budget, similar budget and oversight responsibilities in the implementation of a National Cyber Strategy, to include an annual assessment and report to Congress and the President on departments and agencies' implementation of the strategy and its relevant policies and programs.

The National Cyber Director should have the authority to act as a certifier for department and agency budgets. This authority would grant the National Cyber Director the power to review the annual budget proposal for each federal department or agency and certify to heads of these organizations and the Director of the Office of Management and Budget whether the department or agency proposal is consistent with the National Cyber Strategy. It is expected that the National Cyber Director and the relevant examiners in the Office of Management and Budget would work closely together early and throughout the entire budgetary process to identify inconsistencies, gaps, and redundancies in budget and programs and negotiate resolutions with relevant departments and agencies. Additionally, the Director would have the authority to review department and agency transfer or reprogramming requests to the Office of Management and Budget that would increase or decrease funding for cybersecurity programs, projects, or activities by more than five percent. This authority would allow the Director to ensure transfer and reprogramming actions are also consistent with the National Cyber Strategy.

Defensive Cyber Operations Planning, Coordination, and Execution. The National Cyber Director should lead the coordination and integration of U.S. government defensive cyber activities, such as a Federal government response to a significant cyber incident affecting the U.S. homeland and "defensive cyber campaigns," or whole-of-government efforts designed to deter, defend against, mitigate, or limit the scope of an identified malicious cyber campaign. The National Cyber Director should act primarily as a convening authority in planning and coordinating these operations, ensuring that they are fully integrated, taking full advantage of participating department and agency authorities and capabilities, and reflecting the President's priorities, similar to the authority of the DoD PCA. Day-to-day execution of cybersecurity responsibilities should be carried-out by appropriate federal departments and agencies, such as CISA, the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), Sector Specific Agencies (SSAs), and others as appropriate. The National Cyber Director is intended to ensure that they are appropriately and effectively deconflicted, integrated, and mutually-supporting in their approaches, and receive necessary support in furtherance of

broader government-wide efforts. The DoD PCA, in the authorizing legislation, was granted the authority to assist in the overall supervision of Department defensive cyber operations, including activities of component-level cybersecurity service providers and the integration of such activities with activities of the Cyber Mission Force. Similar to DoD's use of the Chairman Joint Chiefs of Staff (CJCS) position to effect cohesion among the operational COCOM's, the NCD would not serve as the operational commander but would ensure that tasking to the individual agencies is mapped to national strategy, coherent across departments and agencies, mutually supporting, and properly resourced to ensure success.

While the National Cyber Director plays the lead role in coordinating the whole-of-government response to a significant cyber incident, the National Cyber Director should play a supporting role in instances where the incident evolves into a national emergency with broader physical consequences. The Department of Homeland Security, and the Homeland Security Advisor, play leading roles in executing and coordinating government responses for emergencies and disasters. Where these emergencies or disasters are a result of a significant cyber incident, or have caused cyber- or cybersecurity-related consequences of their own, the National Cyber Director would support and coordinate with the Department of Homeland Security and the Homeland Security Advisor within the scope of their authorities and responsibilities.

The Commission recommends that the National Cyber Director be made aware of cyber-related Title 10 and Title 50 operations at the discretion of the National Security Advisor. The NCD, like the PCA at DoD, has a legitimate need for comprehensive situational awareness, and therefore should be given the same insight into offensive operations. Given the complexity of cyber operations, and the potential for retaliation in ways that could affect the homeland, the National Cyber Director should be made aware of relevant U.S. operations in order to plan, coordinate, and balance preparatory defensive efforts with such offensive operations. Furthermore, it is expected that, as a constituent member of the National Security Council, the director would participate in any Principal's Committee meeting where offensive cyber operations are under consideration and provide perspective as appropriate.

Coordination with the Private Sector and International Partners. The National Cyber Director would be the foremost spokesperson for the U.S. government for cybersecurity and emerging technology issues. As an Assistant to the President and the senior-most official in the government focused on cyber and cybersecurity, the National Cyber Director would speak with the President's voice and represent the President's priorities in engagement with the general public, the private sector, and the international community. The National Cyber Director is not intended to overstep or interfere with the traditional roles played by other federal agencies, elements of the Intelligence Community, and others. In any activity where the National Cyber Director engages with the private sector, SLTT leaders, foreign countries, or the general public, it is expected the National Cyber Director would coordinate and work closely with relevant departments and agencies.

The National Cyber Director, and their office, would serve as the principal touchpoint for senior private sector leadership on cyber, cybersecurity, and related emerging technology issues. The National Cyber Director, like the PCA Office for DoD, would complement and coordinate with CISA in developing and building an effective public-private partnership. The Commission recommends that CISA, and other agencies as applicable, include and coordinate with the National Cyber Director in senior-level meetings of sector coordinating councils, cross-sector coordinating councils, and other meetings of the Critical Infrastructure Partnership Advisory Council. The National Cyber Director should also work in conjunction with and complement the Joint Cyber Planning Office (JCPO) within the Cybersecurity and Infrastructure Security Agency, charged with drafting and coordinating plans and playbooks across departments and agencies at the working level under the guidance, processes, and priorities set by the National Cyber Director.[5]

It is expected that the National Cyber Director would participate in meetings with international allies and partners on topics of cybersecurity and emerging technologies to implement the National Cyber Strategy and advance the President's international priorities. The Commission recommends that the National Cyber Director be included as a participant in preparations for and execution of cybersecurity summits and other international meetings at which cybersecurity or related emerging technologies are a major topic.

OTHER NOTABLE RECOMMENDATIONS

CMF Force Structure Assessment: The Commission recommends that Congress direct the Department of Defense (DoD) to conduct a force structure assessment of the Cyber Mission Force (CMF) to ensure appropriate force structure, capabilities, and resources for DoD's numerous missions in cyberspace. The CMF is the operational arm of U.S. Cyber Command, and CMF teams defend the nation in cyberspace, provide support to geographic combatant command, defend the DoD Information Network, as well as serve analysis and planning functions. A force structure assessment of the CMF, as well as an assessment of the resource implications for the various intelligence community agencies that provide tactical intelligence in their capacity as combat support agencies, will work to ensure the CMF has sufficient forces, capabilities, streamlined decision-making processes and appropriately delegated authorities to achieve its objectives.[6]

Vulnerability Assessment of Nuclear Control Systems and conventional weapons programs: A priority of the Commission was developing recommendations to ensure the United States could continue to maintain credible deterrence above the level of war using the full spectrum of DoD response capabilities, and to prevail in crisis and conflict if deterrence fails. This requires the reliability and resilience of our weapons systems–that they will work when needed, and as intended. Our Commission sought to ensure that our adversaries cannot exploit

[5] The Joint Planning Office (JCPO) recommendation is included in only the House FY21 NDAA.
[6] The CMF Force Structure Assessment recommendation is included in both the House and Senate FY21 NDAA.

cyber vulnerabilities to hold our weapon systems, both conventional and nuclear, at risk and that these capabilities are resilient to adversary actions in cyberspace both during conflict as well as below the level of war in day-to-day competition. This is why the Commission recommends that Congress direct the DoD to conduct a cybersecurity vulnerability assessment of all segments of the nuclear control system and continually assess our conventional weapon systems' cyber vulnerabilities. Recently, the DoD has taken critical steps to address this issue. As directed by Congress in the FY2016 NDAA, DoD began assessing the cyber vulnerabilities of each major weapon system. However, barriers to effective cybersecurity remain. There is no permanent process to periodically assess the cybersecurity of fielded systems. Additionally, it is also crucial to evaluate how a cyber intrusion or attack on one system could affect the entire mission, assessing vulnerabilities at a systemic level.[7]

Defense Industrial Base Threat Intelligence Sharing: The Commission recognized that there are gaps in current efforts to address cyber vulnerabilities in the defense industrial base (DIB), where adversary threats continue to cause the loss of national security information and intellectual property. They also generate the risk that, through cyber means, U.S. military systems could be rendered ineffective or their intended uses distorted. This is why one of the critical recommendations the Commission makes in the report is to require companies within the DIB to participate in a threat intelligence sharing program. Today, there is no truly shared and comprehensive picture of the threat environment facing the DIB, and this recommendation works to remedy that.[8]

Delegation of DoD Authorities: The Commission also recommends reviewing the delegation of DoD authorities to ensure they are sufficiently delegated down to enable more rapid decision-making to conduct cyber campaigns. In particular, the Commission recommends a review of the conditions under which information warfare authorities should be delegated to U.S. Cyber Command. While information is not explicitly discussed in the 2018 DoD Cyber Strategy, the Commission recognizes that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making.[9]

Cyber Reserve Force A final critical element of supporting defend forward is the establishment of a "cyber reserve force" to provide a surge capability that the DoD can mobilize in times of crisis or conflict. The Commission believes this should be a non-traditional military reserve force, with less restrictive and burdensome requirements for drilling, grooming, physical fitness, and other standards. This is meant to address issues of talent management, particularly retention, within the current active and reserve force.[10]

---

[7] Vulnerability Assessment of Nuclear Control Systems and conventional weapon systems recommendations are only included in the Senate FY21 NDAA.
[8] DIB Threat Intelligence Sharing recommendation is included in both the Senate and House FY21 NDAA.
[9] Delegation of DoD Authorities recommendation is included in both the Senate and House FY21 NDAA.
[10] The Cyber Reserve Force recommendation is included in both the Senate and House FY21 NDAA.

Threat Hunting: To identify vulnerabilities on networks critical to national security, the Commission also recommends that there should be a mechanism for mandatory threat hunting on DIB networks**.** Actions such as improving detection and mitigation of adversary cyber threats to the DIB are critical to providing for the proper functioning and resilience of key military systems and functions. It is also critical to establish authority for CISA to threat hunt on .gov networks for the same reasons. Congress must also establish authority for CISA to threat hunt on .gov networks. Actions such as improving detection and mitigation of adversary cyber threats to the DIB and the .gov are critical to providing for the proper functioning and resilience of key systems and functions**.**[11]

Joint Cyber Planning Office and Tabletop Exercises: Elements of the U.S. government and the private sector often lack the institutions and tools necessary for successful collaboration to counter and mitigate malicious nation-state cyber campaigns. To address this shortcoming, the executive branch should establish a Joint Cyber Planning Office under CISA to coordinate cybersecurity planning and readiness across the Federal government and between the public and private sectors for significant cyber incidents and malicious cyber campaigns. In a similar vein, Congress should direct the U.S. government to plan and execute a national-level cyber table-top exercise on a biennial basis that involves senior leaders from the executive branch, Congress, state governments, and the private sector, as well as international partners, to build muscle memory for key decision makers, develop new solutions, and strengthen our collective defense.[12]

National Guard: Congress should also clarify the cyber capabilities and strengthen the interoperability of the National Guard. States have increasingly relied on National Guard units under state active duty and Title 32 of the U.S. Code to prepare for, respond to, and recover from cybersecurity incidents that overwhelm state and local assets.[13]

Strategy to Secure Foundational Internet Protocol and Email: To help reduce vulnerabilities in government networks and critical infrastructure, Congress should require the National Telecommunications and Information Administration and CISA to work with private stakeholders to develop a strategy to secure foundational internet protocols. In parallel, CISA should work with private sector partners to implement a more secure standard for email across all U.S.-based email providers.[14]

Continuity of the Economy Planning: The United States must take immediate steps to ensure our critical infrastructure sectors can withstand and quickly respond to and recover from a significant cyber incident. As a whole, the government should more thoroughly plan for what we

[11] The DoD threat hunting recommendation is included in both House and Senate FY21 NDAA, the CISA threat Hunting recommendation is included in only the House FY21 NDAA.
[12] The JCPO and tabletop exercise recommendations are included in only the House FY21 NDAA.
[13] The National Guard recommendation is included in both the Senate and House FY21 NDAA.
[14] The Strategy to Secure Foundational Internet Protocol and Email recommendation is included in only the House FY21 NDAA.

know to be an eventuality, as we currently do for military planning. Congress should direct the executive branch to develop a Continuity of the Economy plan. As the COVID-19 pandemic has demonstrated, the United States does not currently possess sufficient planning to ensure the continuity of the economy in the face of disruption. This plan should include the federal government; state, local, territorial, and tribal (SLTT) entities; and private stakeholders who can collectively identify the resources and authorities needed to rapidly restart our economy after a major disruption. [15]

Codify Sector Risk Management Agencies and Establish a National Risk Management Cycle: The Commission recommends that Congress codify sector-specific agencies in law as "sector risk management agencies" to ensure consistency of effort across critical infrastructure sectors and ensure that these agencies are resourced to meet growing needs. In conjunction with this codification, the Commission recommends establishing a four-year cycle of risk identification and assessment led by DHS, in coordination with sector risk management agencies, that prompts and supports a National Critical Infrastructure Resilience Strategy led by the President.[16]

Joint Collaborative Environment and Integrated Cyber Center: Effectively ensuring U.S. defense in cyberspace also requires creating a robust public-private collaboration to protect national critical infrastructure through sharing and fusing threat information, insights, and other relevant data in a joint collaborative environment. This will require an effective **integrated cyber center** within CISA which will improve integration of the numerous existing federal cybersecurity centers, sustaining and supporting the National Security Agency Cybersecurity Directorate's collaboration with and support to other federal departments and agencies, and facilitate a more robust relationship between the Intelligence Community and the private sector. Such an effort would work hand in hand with the Commission's recommendation to review existing authorities for providing intelligence support to the private sector and, where appropriate, codify processes for identifying private sector cyber intelligence needs and priorities. More generally, it is also critical for Congress to institutionalize DoD participation in public-private cybersecurity initiatives following the model of the Pathfinder program. Such initiatives allow public-private collaboration to move beyond threat information sharing toward better human-to-human collaboration.[17]

Assistant Secretary of State: Congress should create an Assistant Secretary of State in the Department of State, within a new Bureau of Cyberspace Security and Emerging Technologies, who will lead the U.S. government effort to strengthen international norms in cyberspace and build a coalition of like-minded allies and partners to enforce those norms. This high-level leadership is required to coordinate efforts to shape behavior in cyberspace and ensure the future internet reflects the tenets of freedom, interoperability, security, reliability, and openness.

---

[15] The CotE Planning recommendation is included in only the Senate FY21 NDAA.
[16] Codifying Sector Risk Management responsibilities is included in only the House FY21 NDAA.
[17] The Integrated Cyber Center within CISA and funding for a Joint Collaborative Environment recommendations are included in only the House FY21 NDAA.

Not only do these values best support democracy, but they also foster the economic environment in which our open and competitive market thrives.[18]

Cyber Insurance: Insurance could be a means to improve cyber risk management at scale, but the market for insurance to protect against cyber risk is immature and therefore failing to deliver on this public policy potential. To help improve the reliability of cyber insurance risk management and unlock the market, Congress should fund a Federally Funded Research and Development Center to serve as the focal point for the development of training and certification programs for cyber insurance underwriters and claims adjusters.[19]

CONCLUSION

The number of cyberattacks that the United States and its allies and partners have experienced clearly indicate the vulnerabilities we face in defending our critical infrastructure. Today, the nation faces a different challenge in the form of the pandemic, a non-traditional national security emergency, which has demonstrated the critical need we face in the cyber domain for both strategic leadership at the White House, and the need to build resilience in our networks to withstand and rapidly recover from a significant critical infrastructure attack.

We believe this committee, in addition to its traditional DoD oversight responsibilities, should continue to lead in the cyber domain by supporting national security related NDAA cyber provisions, and work to incorporate key Cyberspace Solarium Commission recommendations that strengthen and prepare the nation for cyberattacks, including the recommendations for the National Cyber Director and Continuity of the Economy Planning efforts.

The 2019 NDAA charted the U.S. Cyberspace Solarium Commission to address two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequence? And what policies and legislation are required to implement that strategy? The Commission has completed its assigned tasks and provided the executive branch and Congress with a number of legislative and policy proposals. We now need your leadership to review and enact these key legislative proposals and empower and resource the government and the private sector to prepare ahead of the crisis, and to act with speed and agility to secure our cyber future.

[18] The Assistant Secretary of State recommendation is not included in either the House or Senate FY21 NDAA due to disagreements over where to place the position, not opposition to the concept.
[19] The Cyber Insurance FFRDC recommendation is included in only the House FY21 NDAA.