Testimony of:
The Honorable Angus King,
The Honorable Mike Gallagher,
The Honorable Patrick Murphy,
Mr. Frank Cilluffo

Commissioners of the
Cyberspace Solarium Commission

Before the United States House of Representatives
Committee on Armed Services
Subcommittee on Intelligence and Emerging Threats and Capabilities

"Review of the Recommendations of the Cyberspace Solarium Commission"

July 30, 2020

INTRODUCTION - INTENT OF THE COMMISSION

The Cyberspace Solarium Commission (CSC) was established by the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 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 vigorously 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.

In addressing the NDAA's tasking, the Commission looked at the challenges the nation faces in cyberspace. 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 CHALLENGE

For the last twenty years, adversaries have used cyberspace to attack American power and interests. The more connected and prosperous our society has become, the more vulnerable we are to rival great powers, 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. There are also new industries and services, like cloud computing, which our society relies on for economic growth and is an increasingly critical piece of the broader internet. As we saw last year, hackers do not just target the U.S. government and military personnel—they increasingly target our cities and counties with malware and ransomware attacks.

Securing the nation in the 21st century requires an interconnected system 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 over a hundred million 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 the United States 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 advanced persistent threat groups (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, including temporarily disrupting 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 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 at their most vulnerable state. Remote access and the expansion of the

work-from-home economy continues to increase the threat vectors for criminal actors as the world changes to meet the needs of a global pandemic.

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 and nonstate actors 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**. The public and private sectors, along with key international partners, must collaborate to build resilience and reshape the cyber ecosystem in a manner that increases its security, while imposing costs against malicious actors and preventing attacks of significant consequence.

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 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. It requires international engagement and collaboration with the private sector.

Layered cyber deterrence emphasizes working with the private sector to efficiently coordinate how the nation responds with speed and agility to emerging threats. 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. These three deterrent layers are supported by six policy pillars that organize the 82 recommendations that collectively represent the means to implement our strategy.

RECOMMENDATIONS AND FOCUS OF OUR EFFORT

First, the Commission found that the Federal government lacks consistent and institutionalized leadership, as well as a cohesive, clear strategic vision on cybersecurity. As a result, the Commission recommends that Congress establish a **National Cyber Director** (NCD) in the Executive Office of the President to centralize and coordinate the cybersecurity mission at the national level. The NCD 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 NCD be staffed with approximately 75 to 100 full-time employees, 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. Additionally, the NCD office would support the President by formulating, recommending, integrating, and implementing policies and strategies to improve the nation's ability to operate in cyberspace. The position would provide clear leadership in the White House and signal cybersecurity as an enduring priority in U.S. national security strategy. Additionally, this position would serve as a mechanism to improve effective congressional oversight of this inherently interdisciplinary policy challenge.

Second, 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 the United States has the appropriate force structure and capabilities in cyberspace. Despite having reached full operational capability in 2018, our Commission found that a gap remains between the current CMF and the scale and scope of adversary threats, as well as mission requirements. The CMF is where the bulk of the capabilities exist within the DoD to counter malicious adversary campaigns and impose costs. Currently, the CMF has 133 teams comprising a total of about 6,200 individuals. However, these requirements were determined in 2013, before the United States fully appreciated the scope and scale of the current threat in cyberspace, and before the DoD developed the strategy of defend forward, which has placed additional mission requirements on the CMF. A force structure assessment of the CMF, as well as an assessment of the resource implications for the various intelligence community agencies that serve combat support agency roles, will work to ensure the CMF has sufficient forces, capabilities, and streamlined decision-making processes and authorities to achieve its objectives.

Third, given the improvements in adversary cyber capabilities, the Commission was concerned with ensuring the United States can still 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 that our weapon systems–which form the bedrock of our military advantage and the foundation for deterrence–will work when needed, and as intended. Given

that so much of our military capabilities rest on cyber infrastructure, a priority of our Commission was ensuring that our adversaries cannot exploit cyber vulnerabilities to hold our weapon systems, both conventional and nuclear, at risk and that these capabilities are resilient to adversary actions in cyberspace. 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.** In the Fiscal Year 2016 NDAA, Congress directed DoD to assess the cyber vulnerabilities of each major weapon system. However, gaps remain that must be remediated. For example, there is no permanent process to periodically assess the cybersecurity of fielded systems. Additionally, the current requirement is to assess the vulnerabilities of *individual* weapons platforms. While this is important, it is also crucial to evaluate how a cyber intrusion or attack on one system could affect the entire mission—in other words, to assess vulnerabilities at a systemic level.

Fourth, 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 the Commission recommends Congress request the DoD in 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. 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.

Fifth, 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. The Commission recognizes that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making.

Sixth, 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.

Seventh, the government must continue to improve the resourcing, authorities, and organization of the Cybersecurity and Infrastructure Security Agency (CISA) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience.

The Commission recommends **empowering CISA** with tools to strengthen public-private partnership. Of particular value would be the authorities needed to aid in responding to attempted attacks on critical infrastructure from a variety of actors, ranging from nation-states to criminals. Currently, the U.S. government's authorities in this context are limited exclusively to certain criminal contexts, where evidence of a compromise exists, and do not address instances in which critical infrastructure systems are vulnerable to a cyberattack. To address this gap, Congress should grant **CISA subpoena authority** to enable CISA to more efficiently and effectively notify private and public sector entities put at risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States, while ensuring appropriate liability protections for cooperating private-sector network owners.

Eighth, elements of the U.S. government and the private sector often lack the tools necessary for successful collaboration to counter and mitigate a malicious nation-state cyber campaign. 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 also 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 and develop new solutions and strengthen our collective defense.

Ninth, 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. Resilience against such attacks is critical in reducing benefits that our adversaries can expect from their operations–whether disruption, intellectual property theft, or espionage. As a whole, the government should more thoroughly plan for what we know to be an eventuality, as we currently do in the military domain. Congress should direct the executive branch to develop a **Continuity of the Economy** Plan. This plan should include the Federal government, state, local, tribal, and territorial (SLTT) entities and private stakeholders who can collectively identify the resources and authorities needed to rapidly restart our economy after a major disruption. In addition, the Commission recommends passing a law to endow the Secretary of the Department of Homeland Security with the authority to declare a **Cyber State of Distress** tied to a **Cyber Response and Recovery Fund**, giving the government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical national functions can continue to operate amidst disruption or crisis.

Tenth, 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 partners and allies to enforce those norms. This high-level leadership is required to

coordinate efforts to shape behavior in cyberspace and ensure that values like openness, interoperability, reliability, and security remain an integral part of the future of the internet.

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.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID-19 pandemic has served as a wakeup call for the United States as it both illustrates the challenge of ensuring resilience and continuity in a connected world, and it demonstrates the challenge in responding to non-traditional national security events. It is an example of a crisis that spreads rapidly through the system, stressing everything from emergency services and supply chains to basic human needs. The pandemic has produced cascading effects and high levels of uncertainty. This situation undermines normal policy-making processes and forces decision makers to craft hasty and ad hoc emergency responses in the absence of fulsome preparation and mitigation measures taken well ahead of time. Complex emergencies, like the pandemic, that rely on coordinated action beyond traditional agency responses and processes illustrate what the Commission saw as an acute threat to the security of the United States.

The lessons the country is still learning from the ongoing pandemic are not perfectly analogous to a significant cyberattack, but are highly illustrative of the possible consequences due to similarities between the two types of events. First, both the pandemic and a significant cyberattack are global in nature. Second, both the COVID-19 pandemic and a significant cyberattack require a whole-of-nation response and are likely to challenge existing incident management doctrine and coordination mechanisms. Finally, and perhaps most importantly, **prevention is far cheaper and more effective than response**.

The global health crisis has reinforced the urgency of many of the core recommendations in the Commission's March 2020 report. Responding to complex emergencies will require a balance between response agility and institutional resilience in the economy and critical infrastructure sectors. Preventing and responding to cyber attacks will require strategic leadership and coordination from the highest offices in government, underscoring the importance of a **National Cyber Director**. It relies on a strong understanding of the risks posed by a crisis and a data-driven approach to mitigating those risks before, during, and after a crisis, validating the Commission's recommendations. Specifically, successfully responding to a crisis relies on clear roles and responsibilities for critical actors in the public and private sector as well as

established, exercised relationships and plans, highlighting the importance of **Continuity of the Economy** planning.

CONCLUSION

The United States and its allies and partners have experienced a number of cyberattacks that clearly indicate the need for improved critical infrastructure resilience. Some, like the Dyn DDoS attack in 2016 disabled large portions of our internet, grinding businesses to a halt for several hours. Others, like WannaCry and NotPetya, locked critical institutions out of their systems, placing lives in hospitals at risk and disrupting critical services. Today, the nation faces another wakeup call in the form of the coronavirus crisis, which has provided the clearest depiction yet of a massive disruption of our economy.

The recommendations put forward by the Commission are an important first step to denying adversaries the ability to hold the United States at risk in cyberspace and will be critical to our efforts to re-establish deterrence in cyberspace. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. Cyber operations have become a weapon of choice for adversaries seeking to hold the U.S. economy and national security at risk. Near peer adversaries such as China and Russia are attempting to reassert their influence regionally and globally, using cyber and influence operations to undermine U.S. security interests. The concept of deterrence must evolve to address this new strategic landscape.

Reducing the scope and severity of these adversary cyber operations and campaigns requires adopting the Commission's strategy of layered cyber deterrence to improve our ability to defend our critical infrastructure. To this end, we believe that Congress and the Executive Branch must prioritize a selection of the Commission's recommendations that include: strengthening the government with a National Cyber Director, empowering CISA, creating a new Joint Cyber Planning Office and improving intelligence support to the private sector; while also building resilience with Continuity of the Economy Planning.

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 Congressionally assigned task to develop a new strategic approach, and corresponding legislative proposals. We now need your leadership as you move into conference the 2021 NDAA with your Senate counterparts, in order to enact the critical legislative proposals that will empower and resource the government and the private sector to act with speed and agility to secure our cyber future.