Testimony of:

Senator Angus King,
Representative Mike Gallagher,
Dr. Samantha Ravich,
Ms. Suzanne Spaulding

Commissioners of the
Cyberspace Solarium Commission

Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security of the United States House of Representatives

"Defending Against Future Cyberattacks: Evaluating the Cyberspace Solarium Commission Recommendations"

July 17, 2020

INTRODUCTION - INTENT OF THE COMMISSION AND FOCUS OF OUR EFFORT

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 Cyberspace Solarium Commission consists of fourteen Commissioners, including four currently serving legislators, four executive branch leaders, and six recognized experts with backgrounds in industry, academia, and government service. Senator Angus King and Representative Mike Gallagher serve as the Co-Chairmen. The Commissioners spent the past thirteen months studying the issues, investigating solutions, and deliberating on courses of action to produce a comprehensive report. Our Commissioners convened nearly every Monday that Congress was in session for over a year, achieving an impressive benchmark of 30 meetings. The staff conducted nearly 400 interviews with industry, federal, state and local governments, academia, non-governmental organizations, and international partners. The Commissioners also recruited our nation's leading cybersecurity professionals and academic minds to vigorously stress test the findings and red teamed the different policy options in an effort to distill the optimal approach to securing the United States in cyberspace. The 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 52 legislative proposals that have been shared with the appropriate Committees in the Senate and House of Representatives.

Ultimately, the Commission developed a strategic approach of "layered cyber deterrence" with the objectives of actively shaping behavior in cyberspace, denying benefits to adversaries who exploit this domain, and imposing real costs against those who target America's economic and democratic institutions in and through 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. We believe the future of the U.S. economy and our national security requires both the executive branch and Congress work in tandem to prioritize and grant the following recommendations.

First and foremost, 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, we recommend that Congress establish a **National Cyber Director** in the Executive Office of the President to centralize and coordinate the cybersecurity mission at the national level. The National Cyber Director would work with federal departments and agencies to bring coherence in the development of cybersecurity policy and strategy and in its execution. The position would provide clear leadership in the White House and signal cybersecurity as an enduring priority in U.S. national security strategy.

Second, 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. We recommend **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 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** in support of their threat and asset response activities, while ensuring appropriate liability protections for cooperating private-sector network owners.

Third, 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. Within 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.

Fourth, 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. Congress should direct the executive branch to develop a **Continuity of the Economy** Plan. This plan should include the federal government, 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 establishing 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.

Fifth, the Commission recommends two relevant initiatives to reshape the cyber ecosystem toward greater security for all Americans. The first, the creation of a **National Cybersecurity Certification and Labeling Authority,** would help create standards and transparency that will allow consumers of technology products and services to use the power of their purses over time to demand more security and less vulnerability in the technologies they buy. Furthermore, Congress should appropriate funds to the Department of Homeland Security (DHS), in

partnership with the Department of Energy, Office of the Director of National Intelligence (ODNI), and the Department of Defense (DoD), to competitively select, designate, and fund up to three **Critical Technology Security Centers** in order to centralize efforts directed towards evaluating and testing security of devices and technologies that underpin our networks and critical infrastructure.

Sixth, the U.S. Intelligence Community is not currently resourced or aligned to adequately support the private sector in cyber defense and security. While the intelligence community is formidable in informing security operations in instances when the U.S. government is the defender, its policies and procedures are not aligned to intelligence collection on behalf of private entities, which constitutes around 85% of our critical infrastructure. To that end, Congress should direct the executive branch to conduct a six-month comprehensive review of intelligence policies, procedures, and resources to identify and address key limitations in order to **improve the intelligence community's ability to provide intelligence support to the private sector.**

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 we 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 been a big wakeup call for us all because it illustrates the challenge of ensuring resilience and continuity in a connected world. It is an example of a type of non-traditional national security 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. Complex emergencies 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 several 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. It relies on 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.

THE CHALLENGE

For the last twenty years, adversaries have used cyberspace to attack American power and interests. Our adversaries have not internalized the message that, if they attack us in cyberspace, they will pay a price. 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. As we saw last year, hackers don't just target the U.S. government and military personnel—they increasingly target our cities and counties with malware and ransomware attacks.

Creating a secure nation in the 21st century requires an interconnected system of both public and private networks secure from state and non-state threats. China commits rampant intellectual property theft to help their 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 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.

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 distributed-denial-of-service 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.

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 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 Cyberspace Solarium Commission 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. 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 benefit from targeting 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 fund or 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 contemplates 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.

THE NEED TO REORGANIZE THE U.S. GOVERNMENT (PILLAR 1)

The legislative and executive branches must align their authorities and capabilities to produce the speed and agility required to defend America in cyberspace. Greater collaboration and integration in the planning, resourcing, and employment of government cyber resources between the public and private sectors is a foundational requirement. The U.S. government needs strategic continuity and unity of effort to achieve the goal of layered cyber deterrence called for by the Cyberspace Solarium Commission. These actions require adjusting the authorities and alignment of fundamental processes the U.S. government applies to defend its interests in cyberspace.

First, Congress must reestablish clear oversight responsibility and authority over cyberspace within the legislative branch. The large number of committees and subcommittees claiming some form of jurisdiction over cyber issues is actively impeding action and clarity of oversight. By centralizing responsibility in the new House Permanent Select and Senate Select Committees on Cybersecurity, Congress will be empowered to provide coherent oversight to government strategy and activity in cyberspace.

Next, select entities in the executive branch that deal with cybersecurity must be restructured and streamlined. Multiple departments and agencies have a wide range of responsibilities for securing cyberspace. These responsibilities tend to overlap and at times conflict. The

departments and agencies tend to compete for resources and authorities resulting in conflicting efforts that produce diminishing marginal returns. 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.

In addition to this National Cyber Director, a properly resourced and **empowered CISA** will be critical to achieving coherence in the planning and deployment of government cyber resources. Multiple administrations and Congressional sessions have worked to establish CISA as a keystone of national cybersecurity efforts, but work still needs to be done to realize our ambitious vision for this critical organization. That includes strengthening its director with a five-year term and elevated executive status, adequately resourcing its programs to engage with the private sector while managing national risk, and securing sufficient facilities and required authorities for its vital and growing mission. These changes will remove key limitations in CISA's ability to forge a greater public-private partnership and its mission to secure critical infrastructure.

Finally, the U.S. government must more effectively recruit, develop, and retain a cyber workforce capable of building a defensible digital ecosystem and deploying all instruments of national power in cyberspace. That will require designing innovative programs and partnerships to develop the workforce, supporting and expanding good programs where they are already in place, and connecting with a diverse pool of promising talent. In some cases, success in building a robust federal workforce depends on stakeholders outside the federal government, like educators, non-profits, and businesses. Policymakers should support these important partners by providing the tools they need to be effective, like classroom-ready resources, incentives for research on workforce dynamics, and clear routes for collaborating with the government.

DETERRENCE BY DENIAL (PILLARS 3/4/5)

Denying adversaries' benefits of their cyber campaigns is a critical aspect of "Layered Cyber Deterrence." By ensuring the resilience of critical pillars of national power, reducing our national vulnerability, and disrupting threats through operationalizing collaboration between the government and private sector we can effectively force adversaries to make difficult decisions regarding resourcing, access, and capabilities.The U.S. government support must be better informed through a Joint Collaborative Environment that would pool public-private sources of threat information to be coordinated through a **Joint Cyber Planning Office** and an Integrated Cyber Center at DHS. Paired with our recommendation to conduct a **Biennial National Cyber Tabletop Exercise**, that involves senior leaders from the executive branch, Congress, state governments, and the private sector as well as international partners - the United States and her allies will be in a forward-leaning position and ready to lead.

Today, under the direction of Presidential Policy Directive 21, sector-specific agencies are the lead federal agencies tasked with day-to-day engagement with the private sector on security and resilience. However, there are significant imbalances and inconsistencies in both the capacity and the willingness of these agencies to manage sector-specific risks and participate in government-wide efforts. In addition, the lack of clarity and consistency concerning the responsibilities and requirements for these agencies continues to cause confusion, redundancy, and gaps in resilience efforts. For this reason, 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.

Denying adversaries' benefits starts with ensuring that our most critical targets are able to withstand and quickly recover from cyberattacks. In other words, we must build resilience. Effective national resilience efforts fundamentally depend on the ability of the United States to accurately understand, assess, and manage national cyber risk. Current efforts to assess and manage risk at the national level are relatively new and are significantly hindered by resource limitations, immaturity of process, and inconsistent capacity across departments and agencies that participate in national resilience efforts. Today, while the U.S. government plans for continuity of operations and continuity of government, no similar planning exists to ensure **Continuity of the Economy**. This must change, and the planning process should analyze national critical functions, outlining priorities for response and recovery, and identifying areas for resilience investments. In doing so, the Continuity of the Economy plan should identify areas for preservation of data and mechanisms for extending short-term credit to ensure recovery efforts. Additionally, Congress should also provide CISA with the necessary support to expand its current capability to issue **Cyber State of Distress** declarations in conjunction with **Cyber Response and Recovery Funding**. Furthermore, providing **CISA with Administrative Subpoena Authority** will dramatically improve the federal government's ability to actively notify critical infrastructure owners and operators that are on the front lines and being attacked by our adversaries who are largely acting with impunity.

Denying adversaries' benefits also must lie in driving down our national cyber vulnerability at scale. Today, vulnerability in our cyber ecosystem is derived not only from technology, but also human behavior and processes. The Commission sought means to improve the security of both the technological and human aspects at scale. Moving the technology markets to emphasize security requires creating greater transparency about the security characteristics of technologies consumers buy. This is why the Commission recommends the creation of a **National Cybersecurity Certification and Labeling Authority** and **Critical Technology Security Centers** to collectively to develop and facilitate authoritative, easy to understand security certifications and labels for technology products. By helping consumers make more informed technology purchases, the market will become a difficult place for vendors who do not prioritize security to do business.

DETERRENCE BY SHAPING BEHAVIOR (PILLAR 2)

Layered cyber deterrence includes shaping cyber actors' behavior through strengthened norms of responsible state behavior and non-military instruments of power, such as law enforcement, sanctions, diplomatic engagement and capacity building. A system of norms, based on international engagement and enforced through these instruments of power, helps secure American interests in cyberspace.

To strengthen cyber norms and build a likeminded international coalition to enforce them, the Commission recommends Congress create and adequately resource the Bureau of Cyberspace Security and Emerging Technologies led by an Assistant Secretary of State. The Bureau would bring dedicated cyber leadership and coordination to the Department of State.

Leading internationally also means having strong and coordinated representation in bodies that set global technical standards, therefore, Congress should sufficiently resource the National Institute of Standards and Technology to bolster participation in these bodies. American values, interests, and security are strengthened when international technical standards are developed and set with active U.S. participation. Engaging fully means we must also facilitate robust and integrated participation from across the federal government, academia, civil society, and industry; the U.S. is at its best when we draw input from *all* our experts.

In parallel to robust participation in multilateral bodies, law enforcement activities also provide fruitful ground on which to work with international partners and allies to hold adversaries accountable. We recommend providing the Department of Justice Office of International Affairs with administrative subpoena authority streamlines the Mutual Legal Assistance Treaties process, enabling U.S. law enforcement to help allies and partners prosecute cybercriminals. Additionally, the Commission recommends Congress create and fund 12 additional Federal Bureau of Investigation Cyber Assistant Legal Attachés to facilitate intelligence sharing and help coordinate joint enforcement actions. Investing in these types of international law enforcement activities improve the credibility of enforcement and signal America's commitment to bring malicious actors to justice.

DETERRENCE BY COST IMPOSITION (PILLAR 6)

A key layer of the Commission's strategy outlines how to impose costs to deter malicious adversary behavior and reduce ongoing adversary activities short of armed conflict. As part of this effort, the Commission puts forth two key recommendations: to conduct a force structure assessment of the Cyber Mission Force (CMF); and to conduct a cybersecurity and vulnerability assessments of conventional weapons systems and of the nuclear command, control, and communications enterprise.

Today, the United States has not created credible and sufficient costs against malicious adversary behavior below the level of armed attack—even as the United States has prevented

cyberattacks of significant consequences. Our nation must shift from *responding* to malicious behavior after it has already occurred to *proactively* observing, pursuing, and countering adversary operations. This should include imposing costs to change adversary behavior using all instruments of national power in accordance with international law.

To achieve these ends, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives in and through cyberspace. The CMF is currently considered at full operational capability (FOC) with 133 teams comprising a total of approximately 6,200 individuals. However, these requirements were defined in 2013, well before our nation experienced or observed some of the key events that have shaped our government's understanding of the cyber threat. The FOC determination for the CMF was also well before the development of the Department of Defense's (DoD) defend forward strategy. Therefore, we recommend Congress direct the DoD to conduct a force structure assessment of the CMF to ensure the United States has the appropriate force structure and capabilities in light of growing mission requirements. This should include an assessment of the resource implications for intelligence agencies in their combat support agency roles.

If deterrence fails, the United States must also be confident that its military capabilities will work as intended. However, deterrence across all of the domains of warfare is undermined, and the ability of the U.S. to prevail in crisis and conflict is threatened, if adversaries can hold key military systems and functions, including nuclear systems, at risk through cyber means. Therefore, the Commission recommends Congress direct the DoD to conduct a cybersecurity vulnerability assessment of all segments of nuclear command, control, and communications systems and continually assess weapon systems' cyber vulnerabilities.

Our hope is that, by implementing these recommendations, we can ensure our nation is willing and able to counter and reduce malicious adversary behavior below the level of armed conflict, impose costs to deter significant cyberattacks, and, if necessary, fight and win in crisis and conflict.

CONCLUSION

The recommendations put forward by the Commission are an important first step to denying adversaries the ability to hold America hostage 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 American 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 -- improving our ability to defend our critical infrastructure and investing in an effective public-private collaboration.

To this end, we believe this committee must prioritize a selection of the Commission's recommendations that include: strengthening the government with a National Cyber Director, an empowered CISA, a new Joint Cyber Planning Office, and improved intelligence support to the private sector; building resilience with Continuity of the Economy Planning, and a codified "Cyber State of Distress" tied to a "Cyber Response and Recovery Fund"; and, an improved cyber ecosystem with a National Cybersecurity Certification and Labeling Authority, and the designation of Critical Technology Security Centers.

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 delivered on its mission in the promulgation of "layered cyber deterrence" strategy and the corresponding legislative proposals. We now need your help to enact these key legislative proposals as they will empower the government and the private sector to act with speed and agility in securing our cyber future.