Testimony of:

Senator Angus King,
Representative Mike Gallagher,
Ms. Suzanne Spaulding and
Mr. Tom Fanning

Commissioners of the
Cyber Space Solarium Commission

Before the United States Senate Committee on Homeland Security and Government Affairs

"Report of the Cyberspace Solarium Commission"

May 13, 2020

INTRODUCTION - INTENT OF THE COMMISSION

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."

The Commission consists of fourteen Commissioners, including four serving legislators, four executive branch leaders and six recognized experts with backgrounds in industry, academia, and government service, and Senator Angus King and Representative Mike Gallagher serve as Co-Chairmen. The Commissioners spent the past eleven months studying the issue, investigating solutions, deliberating courses of action, and producing a comprehensive report. The Commission met 29 times in weekly meetings, and the staff conducted nearly 400 interviews with industry, federal, state and local governments, academia, non-governmental organizations, and international partners. The Commission stressed tested its findings and red teamed different policy options in an effort to distill the optimal approach.

The Commission developed a strategic approach of layered cyber deterrence, and identified 82 specific policy or legislative remedies. The legislative recommendations were subsequently turned into 56 legislative proposals that have been shared with the appropriate Senate and House committees. The finished report was presented to the public on March 11, 2020.

Throughout this process the Commission always considered the Congress as its “customer”. Through the NDAA, the Congress tasked teh Commission to investigate the issue of cyber threats that undermine American power and to determine an appropriate strategic approach to protect the nation in cyberspace and identify policy and legislative solutions that protect the nation in cyberspace. We four Commissioners are here today to tell you what we learned, advocate for our recommendations and work with you to assist in any way we can in solving this complex challenge.

FOCUS OF OUR EFFORT

Cyber defense and resilience of the Homeland forms the foundation of the Commission’s strategy. 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 their disruption, minimizing their vulnerability, and disrupting adversary operations that seek to hold them at risk.

First and foremost, the Executive Branch must establish a National Cyber Director to centralize and coordinate the cybersecurity mission at the national level. The National Cyber Director would work among Federal departments and agencies to bring coherence in both 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 greater tools to strengthen public-private partnership, including a Joint Collaborative Environment for real-time information exchange and analysis, an Integrated Cyber Center for person-to-person collaboration, and a Joint Cyber Planning Cell for public-private planning that can be rapidly actioned in a crisis. These changes will forge the type of public-private collaboration necessary to quickly detect, mitigate, and respond and recover from a significant cyber incident.

Third, the United States must take immediate steps to ensure our critical infrastructure can withstand and quickly respond and recover from a significant cyber incident. Resilience against attack is critical in reducing benefits that our adversaries can expect from their operations - whether disruption, intellectual property theft, or espionage. The Commission recommends codifying Sector-specific Agencies as Sector Risk Management Agencies and strengthening their ability to aid critical infrastructure sectors in identifying and managing the risks they face. This work will be critical in establishing a Continuity of the Economy Plan, government-wide and public-private contingency planning to rapidly restart our economy after a major disruption. In addition, we recommend 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.

Finally, the Commission recommends two relevant initiatives to reshape the cyber ecosystem. The first, the creation of a National Cybersecurity Certification and Labeling Authority would help create standards and transparency that overtime will allow consumers of technology products and services to use the power of their purses and demand more security and less vulnerability in the technologies they buy. The second line of effort, the creation of a Bureau of Cyber Statistics, focuses on creating better information to improve the security behavior of individuals and organizations, driving down the human vulnerability that pervades the ecosystem. A fully functioning Bureau of Cyber Statistics would help provide private companies, the public, and government policymakers with an empirical evaluation of what does and does not work in cybersecurity and publish cybersecurity data to inform public policy and cybersecurity investments in the public and private sectors.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID-19 pandemic has been a learning experience for us as it illustrates the challenge of ensuring resilience and continuity in a connected world. It is an example of a type of crisis that spreads rapidly through the system, stressing everything from emergency services and supply

chains to basic human needs. The pandemic produces 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 that eclipses traditional agency responses processes illustrate what the Commission saw as an acute threat to the security of the United States.

The lessons the country is learning from the ongoing pandemic are not perfectly analogous to a significant cyberattack, but are highly illustrative. 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 effort 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 recommendation to codify Sector-specific Agencies and establish a National Risk Management Cycle. Agility in 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 imperative of social distancing during the crisis has brought renewed urgency to digitize critical services and do so securely, stressing the importance of the Commission's recommendation to incentivize the movement to the cloud and broader modernization in state, local, tribal, and territorial governments.

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, 85% of which—according to the U.S. Chamber of Commerce—is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment 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, as we saw in 2019.

Creating a secure Homeland in the 21st century requires a secure interwoven system of both public and private networks from state and non-state threats. China conducts 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 Equifax, Marriott and 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 voter 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. They 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 UN 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 increase in 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

To secure the Homeland in the 21st century requires securing cyberspace. To that end, we propose a new approach: layered cyber deterrence. The strategy combines a number of traditional deterrence mechanisms and extends them beyond the government to develop a whole-of-nation approach. It also updates and strengthens our declaratory policy for cyber attacks 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 national 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 threatening 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 its interests.

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

The Legislative and Executive Branches must better align their authorities and capabilities to produce the speed and agility of action required to defend America in cyberspace. There also needs to be greater collaboration between the public and private sectors in the defense of critical infrastructure and better integration in the planning, resourcing, and employment of government cyber resources. The U.S. government needs strategic continuity and unity of effort if it is going to achieve the goal of layered cyber deterrence called for by the Commission. These actions require adjusting the authorities and alignment of key government processes the 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 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.

Denying adversaries' benefits starts with ensuring that our most critical targets are able to withstand and quickly recover from cyber attacks. 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, 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 codifying sector-specific agencies in law as "Sector Risk Management Agencies", establishing baseline responsibilities and requirements for managing risk in the sector or sectors under their purview, and appropriating necessary funds to carry out their responsibilities. In addition, the Commission recommends that Congress recognize, in law, the lead role of the CISA at the Department of Homeland Security (DHS) in national risk management.

With more robust risk management capability in the federal government, we must also codify the process whereby these agencies come together to provide the federal government with a clearer picture of where we are vulnerable and where we need to place greater resources. The U.S. government has made great strides at understanding national risk through DHS's national critical functions work; however, the U.S. government lacks a rigorous process for identifying, assessing, prioritizing, and ultimately buying down national risk to critical infrastructure. To fill this gap, the Commission recommends that Congress codify a five-year "national risk management cycle" in law to culminate with a "Critical Infrastructure Resilience Strategy" and an accompanying "National Cybersecurity Assistance Fund" to ensure consistent funding for initiatives that underpin or build resilience.

National resilience similarly requires sufficient national capacity and preparedness to respond to and recover from attacks when they do happen. The United States has well-established mechanisms and processes to respond to physical and natural disasters and states of emergencies. The same rigor has not yet been applied to understanding and responding to cyber states of distress and disasters. To address this shortcoming, the Commission recommends Congress pass a law codifying a Cyber State of Distressand and an accompanying Cyber Response and Recovery Fund to assist state, local, tribal, and territorial (SLTT) governments and the private sector beyond what is available through conventional government technical assistance and cyber incident response programs.

Similarly, while Continuity of Operations and Continuity of Government have long been cornerstones of government contingency planning, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major disruption. That is why the Commission recommends that Congress direct the Executive Branch to develop and maintain Continuity of the Economy planning to ensure continuous operation of critical functions of the economy in the event of a significant cyber disruption. 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.

A second major aspect of denying adversaries' benefits lies in driving down our national 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 to develop and facilitate authoritative, easy to understand security certifications and labels for technology products.

Driving down vulnerability in human behavior and processes requires a combination of better emprics to understand what constitutes good cybersecurity behavior and incentives to nudge humans and organizations toward that better behavior. To address the former, the Commission recommends the creation of the Bureau of Cyber Statistics, which would gather relevant data, analyze it, and publish insights for policymakers and the public. Armed with better information about best practices in cybersecurity, policymakers must find a mixture of incentives to encourage individuals and organizations to adhere to them. Insurance is one such incentive.

Although the insurance industry plays an important role in enabling organizations to transfer a small portion of their cyber risk, it is falling short of achieving the public policy objective of driving better practices of risk management in the private sector more generally. Because insurance falls under the purview of state regulators, the federal government can do little to directly affect change in the market for insurance specific to a given industry. Thus, to improve the market for cybersecurity insurance, Congress should appropriate funds and direct DHS to resource a Federally Funded Research and Development Center to develop models for underwriter and claims adjuster training and certification and establish a public-private partnership on modeling cyber risk.

The final aspect of denying adversaries benefits lies in disrupting their operations. Cyber defense, while a shared responsibility, will depend significantly on the underlying efforts of the owners and operators of private networks and infrastructure. The U.S. government and industry thus must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This "collective defense" in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique

comparative advantages for the common defense. This means codifying the "systemically important critical infrastructure" designation for entities responsible for systems and assets that underpin national critical functions, to hold these entities to a higher standard, and to ensure they are fully supported by the U.S. government. Additionally, this 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 Cell and an Integrated Cyber Center at DHS.

DETERRENCE BY SHAPING BEHAVIOUR (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; 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 cyber attacks, and, if necessary, fight and win in crisis and conflict.

CONCLUSION (JENSEN)

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.