CYBERSECURITY LESSONS FROM THE PANDEMIC

CSC White Paper #1

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

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

MAY 2020

EXECUTIVE SUMMARY

The COVID-19 pandemic illustrates the challenge of ensuring resilience and continuity in a connected world. Many of the effects of this new breed of crisis can be significantly ameliorated through advance preparations that yield resilience, coherence, and focus as it spreads rapidly through the entire system, stressing everything from emergency services and supply chains to basic human needs and mental health. The pandemic produces cascading effects and high levels of uncertainty. It has undermined normal policymaking processes and, in the absence of the requisite preparedness, has forced decision makers to craft hasty and ad hoc emergency responses. Unless a new approach is devised, crises like COVID-19 will continue to challenge the modern American way of life each time they emerge. This annex collects observations from the pandemic as they relate to the security of cyberspace, in terms of both the cybersecurity challenges it creates and what it can teach the United States about how to prepare for a major cyber disruption. These insights and the accompanying recommendations, some of which are new and some of which appear in the original March 2020 report, are now more urgent than ever.

The lessons the country is learning from the ongoing pandemic are not perfectly analogous to a significant cyberattack, but they offer many illuminating parallels.

- **First**, both the pandemic and a significant cyberattack can be global in nature, requiring that nations simultaneously look inward to manage a crisis and work across borders to contain its spread.
- **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.
- **Third**, when no immediate therapies or vaccines are available, testing and treatments emerge slowly; such circumstances place a premium on building systems that are agile, are resilient, and enable coordination across the government and private sector, much as is necessary in the cyber realm.
- **Finally**, and perhaps most importantly, prevention is far cheaper and preestablished relationships far more effective than a strategy based solely on detection and response.

This annex highlights the renewed importance of 32 of the Commission's original recommendations and offers four new recommendations in two distinct sections. Section I, **Cybersecurity Challenges during a Pandemic**, focuses on recommendations made more pressing by the pandemic response and associated social distancing protocols. They address several areas, including:

- The **need to digitize critical services** and do so securely, which underscores the importance of stimulus grants to incentivize the movement to the cloud and broader modernization in state, local, tribal, and territorial governments.
- The overall importance of the U.S. government leading the push for a more secure and reliable cyber ecosystem, given **the increase in working from home**.
- The increase in fraud and other malicious activity during the pandemic, which underscores the need to build **capacity to combat opportunistic cybercrime**.

In addition, this section contains two new recommendations:

1. Pass an Internet of Things Security Law
2. Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts

Section II, **What a Pandemic Can Teach the United States about How to Prepare for a Major Cyber Disruption**, focuses on recommendations that the COVID-19 crisis has reinforced as necessary to ensure that the United States is well

positioned to prevent and, if necessary, respond to a crisis induced by a significant cyberattack. Responding to complex emergencies requires a balance between agility and institutional resilience across each sector of the economy, focusing particularly on critical infrastructure. Specifically, this section outlines relevant recommendations pertaining to:

- **Strategic leadership and coordination,** both domestically and internationally, underscoring the importance of the National Cyber Director and a properly resourced Cybersecurity and Infrastructure Security Agency as well as the criticality of establishing a process to ensure Continuity of the Economy planning.
- **Preparedness efforts** led by the government to ensure the availability of critical resources and a workforce ready to aid in response and recovery efforts.
- **Prevention and mitigation efforts** underpinned by a solid foundation of comprehensive data, 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.
- **Response and recovery capability and capacity**, including prior planning and frameworks to coordinate policy responses such as establishing a "Cyber State of Distress" and invoking the Defense Production Act.
- **Capacity to counter disinformation** through societal resilience and organizations that identify, expose, and explain malign foreign influence operations.

In addition, this section contains two new recommendations:

1. Establish the Social Media Data and Threat Analysis Center
2. Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns

Over the past two decades, the United States has experienced a barrage of cyberattacks that have impacted the national economy, American democracy, and peoples' daily lives. Despite these shots across the nation's bow, the United States has been slow to correct our course and update our institutions to meet the threat. Although not a cyberattack, the COVID-19 pandemic serves as another warning shot, challenging the resiliency of the nation in new ways and underscoring the urgency with which the United States must improve its capacity to prevent, withstand, and respond to crises regardless of their cause.

Senator Angus King (I-Maine)
Co-Chairman
Cyberspace Solarium Commission

Representative Mike Gallagher (R-Wisconsin)
Co-Chairman
Cyberspace Solarium Commission

SECTION I: CYBERSECURITY CHALLENGES DURING A PANDEMIC

In addition to offering lessons for cyber crisis management, the COVID-19 pandemic has highlighted the reality that we cannot afford piecemeal resilience in the realm of cyberspace, where the flexibility needed for personal and business operations must not be constrained by an inherent lack of security in its foundations. Social or physical distancing has forced a new reliance on cloud and other technologies that enable remote work and remote services, further underscoring the importance of secure cloud services and of digitization. The need for much of the workforce to work from home has underscored the importance of in-home and consumer information technology devices and a secure and reliable cyber ecosystem. The uptick in opportunistic cybercrime has underscored the importance of ensuring robust law enforcement capabilities and authorities. In some cases, the Commission's recommendations outline a comprehensive approach to addressing these challenges, but the novel circumstances highlight the need to make small modifications to existing recommendations. Other challenges require renewed attention and new ideas.

In this section, the Commission offers two new recommendations on digitizing critical services, supporting the work-from-home economy, and combatting opportunistic cybercrime; it also highlights recommendations from the March 2020 report that are now all the more urgent given the changed conditions created by the pandemic.

A. DIGITIZATION OF CRITICAL SERVICES

The pandemic has produced new requirements that demonstrate the importance of digitizing critical services. During the outbreak, Americans have increasingly relied on federal and state aid programs whose legacy systems have been stressed to the brink of failure. As social distancing has pushed firms to shift their business online, many small and medium-sized businesses—which employ half the population—have been unable to sustain operations. To survive future pandemics or catastrophic cyber incidents, the nation needs secure, remote access to reliable cloud services.[1]

Modernization and digitization, though expensive in the short term, create greater efficiency and flexibility in the delivery of services while reducing spending in the long term. Nonetheless, state, local, tribal, and territorial (SLTT) governments and small businesses, not to mention the federal government, which often struggle to fund basic services, regularly defer digitization in pursuit of shorter-term funding priorities. This short-term trade-off produces long-term consequences. America is now paying the price for decades of short-term thinking.

Digitization of critical services contributes to two positive outcomes. First, it is a key part of resilience as it makes programs more flexible, enabling constituents to receive services remotely in times of both stability and disruption. Second, if done well, digitization can actually serve to improve the security of service providers once responsibility for it is assumed by larger entities, like cloud service providers. Small and medium-sized businesses, as well as state and local entities, gain collective security and economies of scale. Rather than each paying for unique security solutions they pool resources and produce a more defensible, resilient system.

Relevant Recommendation

- **Recommendation 4.5.1 – Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments:** In pursuit of improving both security and capacity to deliver critical services digitally, the Commission proposes a modification to this recommendation. Because the need

to digitize critical state, local, tribal, and territorial government services is urgent, Congress can no longer wait a year for the federal government to study the issue and submit a report. Instead, Congress should include grants to SLTT governments in future COVID-19 stimulus legislation so that these entities can more quickly move to the cloud and modernize their digital infrastructure. Initial payments should be steered toward incentivizing or subsidizing the cost to SLTT governments associated with migrating to cloud infrastructure. These grants should go to state governments and be apportioned based on population. A second tranche of grants focusing on creating digital services should follow and be made available to state, local, tribal, and territorial governments based on a competitive application process. However, the U.S. government cannot let the modernization of infrastructure, though urgent, outpace SLTT governments' ability or need to secure it effectively. The Commission therefore recommends a short-term modification, asking that Congress direct the Department of Homeland Security and the Department of Commerce, in consultation with industry, to identify an existing security standard or set of standards against which the security of cloud services can be measured and which may have to be met to demonstrate eligibility for the grant program.[2]

B. THE WORK-FROM-HOME ECONOMY

The COVID-19 pandemic has been a watershed moment, changing how we live our lives in unexpected ways. The need to socially isolate has forced innovation in how we work, as businesses and governments alike search for ways to maintain the continuity of their operations. The result has been a massive shift to move to remote work, forcing companies to rely on in-home consumer electronics as their employees log in from home. Personal devices and home networks are suddenly a core part of business infrastructure. The internet backbone is now, more than ever, the backbone of our nation's business functions. Yet, as internet traffic surges by 30 to 50 percent,[3] consumer devices and networks provide an easier and larger target and attack surface for our adversaries.[4] At a time when in-person communication and exchange is limited, maintaining the integrity and availability of computing devices and the networks they connect to becomes all the more imperative. As increasing numbers of employees work from home, enterprise IT security operations become less effective—less able to shield devices and infrastructure from compromise and disruption. Businesses are now more reliant on the security of the cyber ecosystem, but they have far less power to mitigate the vulnerabilities and risk that may be introduced.

Relevant Recommendations

- **NEW Recommendation – Pass an Internet of Things Security Law:** With a significant portion of the workforce working from home during the COVID-19 disruption, household internet of things (IoT) devices, particularly household routers, have become vulnerable but important pieces of our national cyber ecosystem and our adversary's attack surface.[5] To ensure that the manufacturers of IoT devices build basic security measures into the products they sell, Congress should pass an IoT security law.[6] The law should focus on known challenges, like insecurity in Wi-Fi routers, and mandate that these devices have reasonable security measures, such as those outlined under the National Institute of Standards and Technology's "Recommendations for IoT Device Manufacturers."[7] But it should be only modestly prescriptive, relying more heavily on outcome-based standards, because security standards change with technology over time. Nonetheless, the law should stress enduring standards both for authentication, such as requiring unique default passwords that a user must change to their own authentication mechanism upon first use, and for patching, such as ensuring that a device is capable of receiving a remote update. Congress should consider explicitly tasking the Federal Trade Commission with enforcement of the law on the basis of existing authorities under Section 5 of the Federal Trade Commission Act.
- **Recommendation 4.1 – Establish and Fund a National Cybersecurity Certification and Labeling Authority:** Creating a National Cybersecurity Certification and Labeling Authority would provide consumers with the information they need to understand the security features of the technology products and services they buy. Our new reality, as parts of our national economy and day-to-day lives have been thrust out of enterprise networks and into personal and in-home devices, underscores the importance of the Commission's recommendations aimed at improving the security

of the technology layer of the cyber ecosystem. The Commission therefore recommends the expedited creation of the proposed National Cybersecurity Certification and Labeling Authority and encourages it to expand the scope of its certification and labeling activities to include consumer and personal electronics as soon as possible.

- **Recommendation 4.2 –- Establish Liability for Final Goods Assemblers:** Holding final goods assemblers of information technology equipment liable for damages from incidents that exploit known vulnerabilities for which no patch has been made available will incentivize them to adopt better patching practices.
- **Recommendation 4.5.2 – Develop a Strategy to Secure Foundational Internet Protocols and Email:** As COVID-19 forces greater dependency on the internet, the reliability and security of the network become even more crucial. Ensuring the security of the core protocols that enable the internet to function is more imperative than ever.

C. THE NEED TO COMBAT OPPORTUNISTIC CYBERCRIME

The uptick in fraud and other malicious activity during the COVID-19 pandemic has provided an unwelcome reminder that major emergencies present opportunities for criminals to further stress overburdened public services and the American people. Cyber threat actors' flagrant conduct during this pandemic reveals that while their tactics and targets have not dramatically changed, they are able to take greater advantage of increasingly vulnerable businesses, governments, and individuals to steal information, defraud their targets, and make Americans feel insecure online. As of April 21, 2020, the FBI's Internet Crime Complaint Center (IC3) reported a tripling of complaints and had reviewed more than 3,600 submissions related to COVID-19 scams.[8] National emergencies like the COVID-19 pandemic can embolden cyber threat actors to aggressively exploit increasingly susceptible victims and security vulnerabilities created and exacerbated by crises. Other areas of U.S. code contain increased penalties for illegal activity that seeks to take advantage of federally declared emergencies, and Congress should explore options to increase criminal penalties for cyber intrusions that exploit national emergencies. Law enforcement plays a crucial role in responding to the increase in cyber threats and criminal activity during national emergencies, and the United States relies on a comprehensive and agile response from investigators and prosecutors to dismantle online schemes and hold cyber threat actors accountable.

Relevant Recommendations

- **Recommendation 1.4.2 – Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force:** Strengthening the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force would provide federal law enforcement with enhanced personnel and resources to conduct and coordinate actions that raise costs for and impose consequences on cyber threat actors. Empowering the FBI's Cyber Division and the National Cyber Investigative Joint Task Force (NCIJTF)—as well as encouraging interagency collaboration by adequately funding all relevant law enforcement agencies, including Department of Homeland Security organizations such as the U.S. Secret Service, to participate in the NCIJTF—would support a robust law enforcement and domestic intelligence response during national emergencies while also enhancing the long-term investigative activities that are central to defending national interests.
- **NEW Recommendation – Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts:** Cyber-specific nonprofit organizations regularly collaborate with law enforcement in writing cybercrime reports, carrying out enforcement operations, and providing victim support services.[9] As the COVID-19 pandemic has proven, trusted nonprofit organizations serve as critical law enforcement partners that can quickly mobilize to help identify and dismantle major online schemes.[10] Such nonprofits have the expertise and flexibility to help and reinforce law enforcement efforts to disrupt cybercrime and assist victims. However, they often face financial challenges.[11] Therefore, the Commission recommends that Congress provide grants through the Department of Justice's Office of Justice Programs to help fund these essential efforts.

SECTION II: WHAT A PANDEMIC CAN TEACH THE UNITED STATES ABOUT HOW TO PREPARE FOR A MAJOR CYBER DISRUPTION

The COVID-19 pandemic has put U.S. crisis leadership, preparedness, response, and recovery to the test. A sufficiently large cyberattack could mirror the virus's effects—widespread disruption of our government, economy, and daily life—with the added challenge that a cyber adversary can watch, learn from, and rapidly adjust to our response. The U.S. government's enormous efforts to respond to and recover from COVID-19 have made obvious the importance of a number of key themes, each of which the Commission has similarly highlighted as important in cybersecurity. First, they demonstrate the importance of dedicated national leadership to coordinate domestically and engage internationally. Second, they highlight the imperative that the entities and individuals most likely to be affected by crises be sufficiently prepared to withstand cyberattacks. Third, they emphasize the need to take a data-driven approach to preventing threats and vulnerabilities and to mitigating consequences. Finally, they underscore the importance of ensuring that the U.S. government has robust plans, authorities, and capacities to respond to and recover from crises. Michael Osterholm, an expert in pandemics, has argued that unlike hurricanes, pandemics are preventable. The same holds true for cyberattacks. As Osterholm asks, "Why wouldn't we want to stop hurricanes before they happen?"[12] Similarly, the Commission asks, "Why wouldn't we want to reduce the severity and frequency of cyberattacks if we could?"

In this section, the Commission highlights recommendations that the COVID-19 crisis has shown are essential in ensuring that the United States can withstand significant cyberattacks and prevent crises. Specifically, we highlight recommendations relevant to leadership and coordination, preparedness, prevention and mitigation, response and recovery, and countering disinformation during a crisis.

A. LEADERSHIP AND COORDINATION PROCESSES

During catastrophic events such as the COVID-19 pandemic or a significant cyberattack, the United States must have a crisis management team and clear strategies in place ahead of time to coordinate an effective response, both at home and abroad. The pandemic has laid bare the limitations and interdependence of both the private sector and the government authorities, highlighting that any successful management of a crisis—cyber or otherwise—will require a coordinated, well-planned, and shared response. The government, the private sector, and the public each have unique and shared responsibilities, and it is during times of calm that these groups must take the measures necessary to ensure their preparedness to quickly and seamlessly respond to a potential crisis. Ensuring that the federal government has clear plans, processes, and capabilities in place before an incident will significantly improve its capacity to aid in response to and recovery from a crisis.

This means that the U.S. government must start putting structures in place to enable leadership and coordination; implementing policies to strengthen the resilience of our economy; developing mechanisms to coordinate quick, effective responses among public and private entities; and laying the groundwork to ensure international coordination.

1. Executive Branch Leadership and Coordination

In confronting COVID-19 or other catastrophes, it is imperative that the executive branch be guided by strong leadership, including subject matter experts who are sufficiently empowered to coordinate, plan, and prepare for a crisis response well ahead of disruptive events. A national response to a significant cyberattack relies on a capable, experienced government

management team with established relationships in the private sector and in state and local governments, as well as on having effective, tested programs, plans, and procedures in place.

Relevant Recommendations

- **Recommendation 1.3 – Establish a National Cyber Director:** Today's circumstances validate the Commission's recommendation for the establishment of a National Cyber Director (NCD), who would act as the President's principal advisor for cybersecurity and related emerging technology issues. As the chief U.S. representative and spokesperson on cybersecurity issues, the NCD would head the development of the national cybersecurity strategy, lead joint interagency planning for the federal government's response activities to cyberattacks, coordinate the federal government's incident response activities, and serve as the focal point for private sector leaders to engage the White House on cybersecurity issues.
- **Recommendation 1.4 – Strengthen the Cybersecurity and Infrastructure Security Agency:** In addition to the institutionalized leadership in the Executive Office of the President, federal agencies must be sufficiently resourced and prepared to lead during times of crisis. The Secretary of Homeland Security plays a critical role in domestic incident management through both the Federal Emergency Management Agency and the Cybersecurity and Infrastructure Security Agency (CISA). CISA must be strengthened to ensure its ability to take a lead role in managing national risk and coordinating the efforts of sector-specific agencies.

2. Planning for Continuity of the Economy

The economic disruption caused by the COVID-19 pandemic illustrates the importance of both understanding how crises may disrupt our national economy and developing plans to ensure its continuity. Resilience through a crisis, regardless of the cause, entails sustaining the United States' core elements of national power. Our system of governance, our military, and our economy each contribute to our national power, and undermining the continuity or effectiveness of any of these pillars of national power during a crisis would weaken the capacity of the nation to withstand and recover from a crisis. The United States has robust planning and procedures to ensure the continuity of operations and government, but it lacks similar planning with regard to the economy. In an increasingly interconnected and competitive global economy, the United States cannot afford to be unprepared for its return to normalcy and must have plans in place to ensure continuity of the economy, in the face of all hazards—not just pandemics and cyberattacks but also other major catastrophic events, such as bioterrorist attacks. The United States' global leadership rests on its economy, the strongest in the world. Disruptions to our national economy, especially during an era of great power competition, enables adversaries to consolidate gains and affords them an opportunity to shift power away from the United States.

Relevant Recommendation

- **Recommendation 3.2 – Develop and Maintain Continuity of the Economy Planning:** To protect the economy during disruptions, the federal government must initiate continuity planning with companies that produce and distribute critical goods and services, before the economy has started to suffer. This planning should include preparatory discussions internally and with core private-sector stakeholders about establishing frameworks and courses of action, maintaining coordinated action, and identifying key single points of failure in the economy that require government protection. Such planning efforts would enable the United States to withstand disruption regardless of cause and ensure the availability and flow of critical goods and services. The Commission's Continuity of the Economy recommendation focuses on ensuring continuity through a cyber disruption, but the United States must ensure the continuous flow of goods and services regardless of the disruption's cause. The COVID-19 pandemic demonstrates how a crisis can enter a worsening spiral, as its economic and logistical consequences make it harder to manage. By getting the right goods and

services to the right places at the right time, Continuity of the Economy planning ensures that the nation maintains its capacity to manage consequences.

3. Quick, Effective, and Coordinated Government Responses

The COVID-19 pandemic has highlighted the importance of preparedness—the "continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response."[13] Preplanning and designing policies years in advance of emergencies enables government and nongovernmental stakeholders to seamlessly implement those policies and procedures in a crisis. In a time of crisis, getting policy right is only one part of the equation; prior planning, clearly defined roles and responsibilities, and coordination build the foundation required to make smart leadership and seamless response possible. Planning and coordination in and between the government and the private sector are essential for ensuring that businesses and governments remain resilient and ready to participate in the larger national response and recovery efforts. The United States government must bolster its planning and coordination mechanisms to ensure a quick and effective government response.

Relevant Recommendations

- **Recommendation 5.4 – Establish a Joint Cyber Planning Cell under the Cybersecurity and Infrastructure Security Agency:** A Joint Cyber Planning Cell would facilitate development of plans for coordinated action between the government and the private sector under the direction of CISA. Given its mandate to plan whole-of-government, public-private cyber defense and security campaigns, the Joint Cyber Planning Cell would be well equipped to respond quickly, without needing to build comprehensive policies and develop processes during a major event.
- **Recommendation 3.3.3 – Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts:** Expanding planning capacity within the Department of Homeland Security would bolster the nation's planning efforts and clarify roles and responsibilities before the crisis hits, further streamlining coordinated decision making. These efforts would be complemented by Commission recommendations to **conduct cyber exercises for all relevant stakeholders** (recommendations 3.3.4 and 3.3.5).

4. International Coordination

Both cyber and pandemic crises are inherently cross-border problems, and any U.S. effort to contain and combat them will require significant cooperation and collective action with the international community. Strong norms and international engagement are critical for shaping behavior, preventing further harm, and stabilizing the environment during a crisis through the creation of shared expectations and understandings. In the absence of credible enforcement of these norms, critical infrastructure becomes even more vulnerable in a crisis, as is currently shown by state-sponsored hacking operations against U.S. health care infrastructure, including against institutions that are conducting research into COVID-19 vaccines and treatments.[14] Right now, these state-sponsored exploitations appear mainly to be gathering information on medical data. However, in the midst of global crisis, if operations of this nature expand or become more destructive, they could strain already scarce resources and result in loss of life. Thus, the current COVID-19 pandemic demonstrates the critical need for international cyber leadership.

Relevant Recommendations

- **Recommendation 2.1 – Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State:** Strong State Department leadership is critical for coordinating an international response to a crisis. To fill this gap in the context of cybersecurity, the Commission recommends the creation of the Bureau of Cyberspace Security and Emerging Technologies (CSET) within the U.S. Department of State, led by an Assistant Secretary of State.

- **Recommendation 2.1.1 – Strengthen Norms of Responsible State Behavior in Cyberspace:** Strong norms are critical for shaping behavior, preventing further harm, and stabilizing the environment during a crisis. Once established, CSET would work with international partners to strengthen and implement international norms for responsible state behavior in cyberspace.
- **Recommendation 2.1.3 – Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance:** In the absence of credible enforcement of these norms, critical infrastructure becomes even more vulnerable in a crisis, as is currently the case with state-sponsored hacking operations against health care critical infrastructure that are targeting U.S. institutions conducting research into COVID-19 vaccines and treatments.[15] State Department efforts to build capacity in partner nations are all the more relevant in order to prevent these types of operations.

B. PREPAREDNESS

To ensure that the United States is properly prepared for a major crisis such as the COVID-19 pandemic or a significant cyberattack, the U.S. government must take steps to make certain that the nation has the resources necessary to respond to and recover from a crisis and that our core democratic institutions are not unduly disrupted by such a crisis. In the context of a pandemic, this means ensuring the availability of critical medical supplies and ensuring a well-prepared and well-maintained medical workforce. For a significant cyberattack, those critical resources could take the form of either information technologies or components required to reconstitute critical systems or the cybersecurity services or expertise needed to respond to and recover from incidents.

To ensure that the United States is prepared for significant cyberattacks, the U.S. government must take steps to identify and secure the availability of critical resources, grow a robust and competent cybersecurity workforce, and implement safeguards for our elections.

1. Availability and Security of Critical Resources

The COVID-19 crisis has reinforced the importance of understanding and mitigating supply chain dependencies and shortfalls in domestic production capacity to protect businesses from crises and shocks that disrupt international flows of goods and services. In the COVID-19 crisis, shocks have resulted in shortages of medical supplies. In a cyber crisis, they could manifest in the form of shortages in vital microchips or radio equipment needed to rebuild critical systems following a failure. Importantly, one key difference between a cyber crisis and a pandemic is in the roles played by compromised critical resources. In a pandemic, the unavailability or insecurity of critical resources hinders response, whereas in a cyber crisis, compromised components such as microchips or radio equipment can themselves be the root cause of the catastrophe.

Relevant Recommendations

- **Recommendation 4.6 – Develop and Implement an Information and Communications Technology Industrial Base Strategy:** In the U.S. system—a market economy and free society—the government's power to direct resources grows markedly during a crisis; but the shortages of critical resources during the COVID-19 pandemic have validated the Commission's finding that the United States must do more to ensure that the necessary resources are available before a crisis. Developing and implementing an information and communications technology industrial base strategy to identify critical dependencies and to direct strategic investments will ensure the industrial capacity needed to alleviate those critical dependencies.
- **Recommendation 3.3.1 – Designate Responsibilities for Cybersecurity Services under the Defense Production Act:** Defense Production Act (DPA) authorities can be leveraged by the federal government to prioritize contracts in a time of crisis, as its use of DPA authorities to contract 3M to produce more N95 respirator masks as part of the COVID-19 pandemic response showed;[16] and during a cyber crisis they could enable the federal government to allocate

critical cyber incident response services. However, even earlier—during the planning process to understand market gaps—the federal government should draw on DPA authorities to help catalyze domestic production of critical information and communication technologies and components so that critical resources will be available should foreign supply chains be disrupted.

2. A Robust Federal Cybersecurity Workforce

The COVID-19 crisis has underscored the importance of building a capable workforce to manage the outbreak of a crisis in both the public and private sectors. During the COVID-19 pandemic, the United States has relied heavily on its doctors, nurses, and disease control experts. Following a significant cyberattack, the United States will need to rely on a skilled cybersecurity workforce. The COVID-19 crisis has pushed tens of millions of Americans out of work, yet tens of thousands of cybersecurity jobs remain unfilled in the public sector alone. While retraining or upskilling workers recently laid off from other fields could take years of development, now is the time to invest in on-the-job training programs and apprenticeships that can make this development a reality. In doing so, the federal government will begin to fill a critical capacity gap while providing a proof of concept to spur similar development in the private sector and among SLTT governments.

Relevant Recommendation

- **Recommendation 1.5 – Diversify and Strengthen the Federal Cybersecurity Workforce:** Congress should immediately authorize additional flexibility to use direct hire authorities as necessary in order to allow federal agencies to determine the appropriate candidates for these in-demand vacancies. Congress should further provide the funding required to foster the development of high-quality programs. The Commission's recommendation should be revised to emphasize that with these new authorities and funding, federal agencies should rapidly develop and deploy apprenticeship programs for cyber roles focused on reskilling unemployed Americans to fill critical cybersecurity workforce gaps. Direct hire authorities across agencies should be deployed to their fullest potential, without the often problematic bureaucratic checklists typical of federal government hiring. The federal government should target not just senior positions but also entry-level positions to attract and hire early career, trainable talent. Apprenticeship programs registered by the Department of Labor or state apprenticeship agencies can provide pathways into long-term cyber careers, drawing on the experience of communities of practice such as the National Initiative for Cybersecurity Education's Sub-Working Group on Apprenticeships.

3. Voter Safety and Secure, Credible Voting

The imperative of social distancing thrust on Americans by the COVID-19 crisis has challenged many of our core institutions, perhaps none more seriously than our elections. American democracy depends on elections occurring on a fixed schedule. Because of the certainty of our election timelines and the uncertainty in our environment, the federal government must have the capacity to quickly surge federal expertise and resources in support of elections. The Commission agrees with experts on both sides of the aisle who acknowledge the technical and practical limitations that make secure online voting impossible at this time,[17] but the COVID-19 pandemic has highlighted the need for an accessible, secure, credible, remote voting capability that is available to portions of the American public, should in-person voting be limited when a primary or election day arrives. Given the decentralized administration of our elections, balancing risk and finding a solution should, as is always the case in American democracy, be done by those closest to the voters: state and local election officials. For this reason, it is imperative that these election officials be empowered with expert advice and have access to financial resources to implement changes on such a short timetable. As state and local election officials work to find solutions, it is essential that the civil rights of every American eligible to vote are upheld.

Relevant Recommendation

- **Recommendation 3.4 – Improve the Structure and Enhance Funding of the Election Assistance Commission:** The Election Assistance Commission (EAC) is the federal entity designated to meet these challenges, but to do so it must be strengthened and better resourced. As the national clearinghouse and resource for information on election administration, the EAC has the necessary expertise in disbursing grants to states that would allow the EAC to find solutions and funding to address states' election challenges. It also has the expertise in election administration and the relationships necessary within the federal government and with the states to navigate risk assessment and mitigation and crisis response, so that state and local election officials can be empowered in their administration of our elections.

C. PREVENTION AND MITIGATION

The COVID-19 pandemic and the myriad other crises over the past several decades have exposed the U.S. government's systemic underinvestment in prevention and mitigation measures for national security events outside the realm of the military. While that assertion holds true broadly, it is particularly applicable in the context of cybersecurity, where national risk assessment and management efforts are nascent and consistent funding to address identified risks has not been established. Prevention and mitigation activities are crucial before a crisis both to decrease the likelihood of it occurring in the first place and to diminish its potential consequences if it does occur. Thus the necessary data must be gathered to understand two key variables of risk—vulnerability and threat—and measures taken to reduce both. Mitigation addresses the third variable of risk—consequence—and focuses on minimizing the impact of a disaster or crisis.

To better prevent attacks and mitigate their consequences, the United States must engage in sustained national risk assessment and management and take a data-driven approach to understanding cybersecurity and cyber risk.

1. Sustained National Risk Assessment and Management

The COVID-19 crisis has underscored the importance of continually assessing risk and prioritizing prevention efforts. Critical infrastructure sectors tend to be interdependent. A shock to one can cascade through the system and quickly disrupt core elements of national power. Whether that shock be caused by a pandemic or a significant cyberattack or something else, understanding risk events and how they might affect multiple critical infrastructure sectors helps officials develop response plans and build in prevention mechanisms that increase resiliency. This process works best in collaboration with the private sector, which owns and operates most of the critical infrastructure in the United States.

Sector-specific agencies (SSAs) and CISA are the crucial government entities that assist private-sector entities in identifying and managing the risks to their enterprise and the systemic risks to other critical infrastructure sectors if their businesses are disrupted or compromised. Furthermore, the COVID-19 crisis has demonstrated the extreme financial and material costs of responding ad hoc to a systemic risk event after the fact. From pandemics and climate shocks to natural disasters and cyber incidents, the systemic risk events on the horizon are increasing and require a more proactive government response. The United States can no longer afford piecemeal responses that are too late to contain the damage inflicted by a major disruption on the networks and infrastructure on which Americans rely. The nation must invest in systems that better forecast, rank, and manage risk now. The resulting ability to anticipate future dangers will help decision makers prioritize scarce resources and increase resilience.

Relevant Recommendations

- **Recommendation 3.1 – Codify Sector-specific Agencies into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk:** The wide disparities in both the capacity and

the willingness of SSAs to work within their sectors and participate in governmentwide efforts must be addressed by codifying these agencies in law as Sector Risk Management Agencies (SRMAs). By establishing basic expectations and responsibilities for these agencies, this effort would provide the foundation for greater resources, authority, and accountability. A **strengthened CISA (recommendation 1.4)** is crucial both for ensuring robust SRMA coordination and for leading national risk management efforts by continuing the National Risk Management Center and National Critical Functions work.

- **Recommendation 3.1.1 – Establish a Five-Year National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy:** Together, SRMAs and CISA should develop a Critical Infrastructure Resilience Strategy underpinned by a five-year national risk management cycle.
- **Recommendation 3.1.2 – Establish a National Cybersecurity Assistance Fund to Ensure Consistent and Timely Funding for Initiatives That Underpin National Resilience:** While the U.S. government has funds to resource disaster prevention and preparedness broadly, no such dedicated fund exists for cybersecurity resilience efforts. A National Cybersecurity Assistance Fund, intended for projects and programs that address clearly defined critical risk where market forces cannot or will not provide sufficient incentive for private action, would address this shortcoming. Opportunities and priorities for investment should be identified through a national risk management cycle and a critical infrastructure resilience strategy.

2. The Critical Need for Data

The COVID-19 crisis has illuminated the challenges of crafting meaningful risk management and mitigation programs without accurate data and forecasts. A lack of resources to model how the spread of the disease could intersect with other points of fragility across critical infrastructure sectors has limited the ability of decision makers to get ahead of the crisis. The United States cannot meaningfully prevent, manage, or mitigate future pandemics or significant cyberattacks if it lacks data, forecasts, and scenarios that visualize and describe systemic risks. The United States must therefore invest in resources that help policymakers understand the new breed of crises likely to threaten Americans in the 21st century.

Relevant Recommendations

- **Recommendation 2.1.6 – Improve Attribution Analysis and the Attribution-Decision Rubric:** Improving attribution analysis and developing an attribution-decision rubric would provide policymakers with important information on who is causing an incident or crisis, helping them to formulate a comprehensive response.
- **Recommendation 4.3 – Establish a Bureau of Cyber Statistics:** In the context of cybersecurity, the U.S. government must bolster its capacity to take in data, share it with relevant stakeholders in critical infrastructure entities, and make it available to the research community. Establishing a Bureau of Cyber Statistics would create a central capacity empowered to collect and provide statistical data, including data on cyber threats, cyber crime—in consultation and collaboration with ongoing efforts by the Bureau of Justice Statistics—and the cyber ecosystem to inform policymakers, the private sector, the general public, and the research community.
- **Recommendation 4.4.1 – Establish a Public-Private Partnership on Modeling Risk:** A public-private partnership on modeling cyber risk would further institutionalize and provide resources for private research efforts in this area.
- **Recommendation 5.2 – Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information:** Establishing a Joint Collaborative Environment to fuse threat information and insight would ensure the continual collection and dissemination of relevant data and metrics to owners and operators of critical infrastructure. The environment would be enabled by data collected through a **national cyber incident reporting law (recommendation 5.2.2)** and a **national data breach notification law (recommendation 4.7.1)**, as well as data collected via **expanded and standardized voluntary threat detection programs (recommendation 5.2.1)**.

D. RESPONSE AND RECOVERY

Although the United States must invest aggressively in preparedness, prevention, and mitigation, the COVID-19 pandemic has shown that crises can still occur, despite the nation's best efforts at preventing them. To prepare for these eventualities, the U.S. government must possess the capacity, capability, and authority to launch swift and comprehensive responses to crises, in coordination with the private sector. While the COVID-19 response has demonstrated the U.S. government's ability to creatively leverage existing authorities in new contexts, Congress should endow the executive branch with both the funding and the authorities to participate meaningfully in responding to and recovering from a significant cyberattack.

1. Government Capacity to Respond to Crises

The COVID-19 pandemic has shown that the impact of a crisis varies according to the scope, scale, and speed of the response taken by different governments. The federal government must have the authorities and resources necessary to manage a crisis and mitigate potential damage before it reaches a state of emergency. Current authorities for cyber incident response, outlined under Presidential Policy Directive 41 and detailed in the National Cyber Incident Response Plan, do not sufficiently empower federal agencies to respond to a significant cyberattack, even after the "significant cyber incident" designation has been made. In addition, these authorities do not provide additional resources and funding. The absence of sufficient resources to manage significant cyber incidents remains a hindrance to the U.S. government's ability to respond comprehensively to significant cyberattacks.

Relevant Recommendations

- **Recommendation 3.3 – Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund":** Most cyberattacks will fall below the threshold for a national emergency declaration. The Commission recommends the creation of a "Cyber State of Distress," a federal declaration that would trigger the availability of additional resources through a "Cyber Response and Recovery Fund." The fund would allow for rapid mobilization and deployment of resources to assist governments and the private sector beyond what is available through conventional technical assistance and cyber incident response programs.
- **Recommendation 3.3.6 – Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard** and **Recommendation 6.1.7 – Assess the Establishment of a Military Cyber Reserve:** A robust military cyber reserve, together with clarified and strengthened interoperability of the National Guard, would provide an enduring latent surge capacity that could be rapidly mobilized in a time of crisis.

E. COUNTERING DISINFORMATION

The current crisis has highlighted the importance of the U.S. population's ability to separate fact from fiction in order to allay fear and save lives. In the months since the initial outbreak of COVID-19, disinformation has reared its ugly head, sowing confusion and doubt among the public about authoritative guidance for protection against the pandemic. Making trustworthy information available to the public is key to preventing adversary cyber-enabled disinformation operations from jeopardizing our ability to respond during a crisis. Left unaddressed, disinformation operations enable adversaries to achieve their goals of creating discord while artificially improving their international standing. Our adversaries' disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts with which Americans are best acquainted. Indeed, these campaigns are menacing the reliability of our public health discourse. The resulting confusion is threatening to become a literal matter of life and death.

Building societal resilience to disinformation presents the most effective and sustainable way to defeat disinformation campaigns in the long term, but Americans also need tools to help identify urgent and acute threats posed by such campaigns in the midst of a crisis. Here the Commission underscores the importance of prior recommendations to build societal

resilience and offers two new recommendations to help build national, nongovernmental capacity to identify and counter disinformation.

1. Creating Societal Resilience to Disinformation

The disinformation surrounding the COVID-19 response has further underscored the importance of building societal resilience to disinformation. Currently, China is utilizing disinformation to cloud the public's view of the origins of the COVID-19 pandemic and the number of cases in China.[18] A European Union watchdog has found 80 instances in which Russia fabricated and exaggerated conspiracy theories about the pandemic, including claims that the virus was a biological weapon or hoax, as well as false reports on the origins of the virus and on the health of foreign leaders.[19] Our adversaries use information operations to deepen fissures within society and between the governed and their government, exploiting and exacerbating declining trust in institutions. One goal of disinformation is to convince the public that the system, whether political or—as with the pandemic—governance, is irrevocably broken. Effective civics education teaches not just that there are three branches of government, but the role of democratic institutions and the role of the individual in sustaining democracy. This understanding can build resilience against pernicious messaging designed to erode the informed and engaged citizenry upon which democracy depends. As the Commission notes, quoting Joseph S. Nye, "The defense of democracy in an age of cyber information war cannot rely on technology alone."[20] Americans must become better equipped to recognize such operations, so that they will be less susceptible to them.

Relevant Recommendation

- **Recommendation 3.5 – Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations:** Through digital literacy and modernized civic education, the U.S. government can assist in enhancing the average American's ability to discern the trustworthiness of online content, and thereby reduce the impact of malicious foreign cyber-enabled information campaigns, without running afoul of concerns about regulating speech. The Commission also recommends that the United States evaluate and strengthen efforts to raise public awareness of cyber threats. Among other problems, disinformation about the pandemic has caused confusion about the spread of the virus, creating varying levels of adherence to recommendations by the Centers for Disease Control and Prevention to prevent it. Building better societal resilience through public education and digital literacy efforts will help the United States avoid making the same mistake with future adversary disinformation operations.

2. Identifying and Countering Disinformation

As the damage caused by COVID-19-related disinformation makes clear, in addition to undertaking long-term public education initiatives, it is imperative that the United States possess the capacity to identify highly dangerous disinformation activities and make them known both to the platforms that enable the activities and to the general public. The Commission therefore believes that civil society must also maintain a robust nongovernmental capability to identify these disinformation activities and their malign infrastructure. Democratic governments must continue to shun any inclination to become arbiters of truth, but it *is* critical that the U.S. government help ensure that social media companies, other media outlets, and stakeholders in the private sector and civil society continue building the expertise and credibility necessary to sound the alarm when disinformation campaigns pose an urgent threat to the American public.

Relevant Recommendations

- **NEW Recommendation – Establish the Social Media Data and Threat Analysis Center:** Because major social media platforms are owned by private companies, developing a robust public-private partnership is essential to effectively combat disinformation. To this end, the Commission supports the provision in the FY2020 National Defense Authorization Act that authorizes the Office of the Director of National Intelligence to establish and fund a Social Media Data and

Threat Analysis Center (DTAC),[21] which would take the form of an independent, nonprofit organization intended to encourage public-private cooperation to detect and counter foreign influence operations against the United States. The center would serve as a public-private facilitator, developing information-sharing procedures and establishing—jointly with social media—the threat indicators that the center will be able to access and analyze. In addition, the DTAC would be tasked with informing the public about the criteria and standards for analyzing, investigating, and determining threats from malign influence operations. Finally, in order to strengthen a collective understanding of the threats, the center would host a searchable archive of aggregated information related to foreign influence and disinformation operations.

- **NEW Recommendation – Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns:** Congress should fund the Department of Justice to provide grants, in consultation with the Department of Homeland Security and the National Science Foundation, to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public while putting those campaigns in context to avoid amplifying them. Such malign foreign influence campaigns can include covert foreign state and non-state propaganda, disinformation, or other inauthentic activity across online platforms, social networks, or other communities. These centers should analyze and monitor foreign influence operations, identify trends, put those trends into context, and create a robust, credible source of information for the American public. To ensure success, these centers should be well-resourced and coordinated with ongoing government efforts and international partners' efforts.

CONCLUSION

As Commission Co-Chairs Senator Angus King and Representative Michael Gallagher have noted, the goal of the Cyberspace Solarium Commission is to be like the "9/11 Commission without the 9/11 event." The COVID-19 pandemic is a call to action to ensure that the United States is better prepared to withstand shocks and crises of all varieties, especially those like cyber events that we can reasonably predict will occur, even if we do not know when. We, as a nation, must internalize the lessons learned from this emergency and move forward to strengthen U.S. national preparedness. This means building structures in government now to ensure strategic leadership and coordination through a cyber crisis. It means driving down the vulnerability of the nation's networks and technologies. And finally, it means investing in rigorously building greater resiliency in the government, in critical infrastructure, and in our citizenry. In the past several years, experts have sounded the alarm, ranking cyberattacks as one of the most likely causes of a crisis.[22] As the COVID-19 crisis has unfolded, the United States has experienced a wake-up call, prompting a national conversation about disaster prevention, crisis preparedness, and incident response. While COVID-19 is the root cause of today's crisis, a significant cyberattack could be the cause of the next. If that proves to be the case, history will surely note that the time to prepare was now.

NOTES

1 In this context, we use the term "cloud services" to refer to a wide range of services delivered on demand to companies and customers over the internet, including software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).

2 The Commission emphasizes that the National Cybersecurity Certification and Labeling Authority or the Department of Homeland Security, in coordination with the Department of Commerce, must develop an authoritative cloud security certification in tandem with funding for cloud services.

3 John Graham-Cumming, "Internet Performance during the COVID-19 Emergency," *Cloudflare*, April 23, 2020, https://blog.cloudflare.com/recent-trends-in-internet-traffic/; Will Douglas Heaven, "Why the Coronavirus Lockdown Is Making the Internet Stronger Than Ever," *MIT Technology Review*, April 7, 2020, https://www.technologyreview.com/2020/04/07/998552/why-the-coronavirus-lockdown-is-making-the-internet-better-than-ever/.

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

5 For the purposes of this annex, we use the definition for "internet of things" adopted by the ISO/IEC: "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react" (ISO/IEC JTC 1, "Internet of Things (IoT): Preliminary Report 2014," 3, https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf). These devices, in general, are hardware with limited functionality, limited user interface, and limited software—for example, connected industrial control systems and household routers.

6 The proposed Internet of Things (IoT) Cybersecurity Improvement Act of 2019 provides a viable model for a federal law that mandates that connected devices procured by the federal government have reasonable security measures in place, but should be expanded to cover all devices sold or offered for sale in the United States. For more, see Internet of Things Cybersecurity Improvement Act of 2019, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/734.

7 Michael Fagan, Katerina N. Megas, Karen Scarfone, and Matthew Smith, "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline," Draft 2, NISTIR 8259, National Institute of Standards and Technology, January 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf.

8 These schemes often use phishing emails and malicious websites; for example, they promote fake vaccines and cures, fraudulent charity drives, and false information on government aid—while at the same time delivering malware to unsuspecting users. Even as adversary nations themselves grapple with the crisis, they apparently are seeking to exploit it to exert geopolitical pressure and to steal institutions' vaccine and treatment breakthroughs. For more information, see "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," U.S. Department of Justice, April 22, 2020, https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams.

9 "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," U.S. Department of Justice, May 23, 2018, https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected.

10 "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams."

11 "Saving Shadowserver and Securing the Internet—Why You Should Care & How You Can Help," *ShadowServer*, March 16, 2020, https://www.shadowserver.org/news/saving-shadowserver-and-securing-the-internet-why-you-should-care-how-you-can-help/.

12 Stephanie Soucheray, "Osterholm Plays Detective, General in 'Deadliest Enemy' Book," Center for Infectious Disease Research Policy, March 14, 2017, https://www.cidrap.umn.edu/news-perspective/2017/03/osterholm-plays-detective-general-deadliest-enemy-book.

13 "Prevention & Preparedness Resources," U.S. Department of Homeland Security, FEMA, https://training.fema.gov/programs/emischool/el361toolkit/preventionresources.htm.

14 Raphael Satter and Christopher Bing, "FBI Official Says Foreign Hackers Have Targeted COVID-19 Research," *Reuters*, April 16, 2020, https://www.reuters.com/article/us-health-coronavirus-cyber/fbi-official-says-foreign-hackers-have-targeted-covid-19-research-idUSKBN21Y3GL.

15 Satter and Bing, "FBI Official Says Foreign Hackers Have Targeted COVID-19 Research."

16 Donald J. Trump, "Memorandum on Order under the Defense Production Act Regarding 3M Company," April 2, 2020, The White House, https://www.whitehouse.gov/presidential-actions/memorandum-order-defense-production-act-regarding-3m-company/.

17 Ian Chipman, "David Dill: Why Online Voting Is a Danger to Democracy," *Stanford Engineering Magazine*, June 3, 2016, https://engineering.stanford.edu/magazine/article/david-dill-why-online-voting-danger-democracy; David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online?," *Verified Voting*, accessed March 24, 2020, https://www.verifiedvoting.org/resources/internet-voting/vote-online/; AJ Vicens, "Online Voting Is a Really, Really Bad Idea," *Mother Jones*, November 9, 2019, https://www.motherjones.com/politics/2019/11/online-voting-problems/; Hans von Spakovsky, "The Dangers of Internet Voting," *The Heritage Foundation*, July 14, 2015, rev. and updated July 26, 2016, available at https://www.heritage.org/report/the-dangers-internet-voting.

18 Jed Babbin, "China and Russia Play COVID-19 Pandemic Disinformation Games," *Washington Times*, April 6, 2020, https://www.washingtontimes.com/news/2020/apr/6/china-and-russia-play-covid-19-pandemic-disinforma/.

19 Jennifer Rankin, "Russian Media 'Spreading Covid-19 Disinformation,'" *The Guardian*, March 18, 2020, https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation.

20 Joseph S. Nye, "Protecting Democracy in an Era of Cyber Information War" (Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2019), 14, https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf.

21 "National Defense Authorization Act for Fiscal Year 2020," Pub. L. No. 116-92, § 5323(c), (f) (2019), 116th Congress, https://www.congress.gov/bill/116th-congress/senate-bill/1790.

22 See, for example, World Economic Forum, *The Global Risks Report 2020* (Geneva: World Economic Forum, January 15, 2020), http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf, and Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community" (Office of the Director of National Intelligence, January 29, 2019), https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

COMMISSIONERS

CO-CHAIRMEN

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

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

COMMISSIONERS

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

Andrew Hallman, Principal Executive of the Office of the Director of National Intelligence performing the duties of the Principal Deputy Director of National Intelligence

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

James R. "Jim" Langevin, U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

David L. Norquist, Deputy Secretary of Defense

David Pekoske, Administrator of the Transportation Security Administration

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Christopher Wray, Director of the Federal Bureau of Investigation

STAFF

SENIOR STAFF
Mark Montgomery, Executive Director
Deborah Grays, Chief of Staff
Erica Borghard, Senior Director and Task Force One Lead
John Costello, Senior Director and Task Force Two Lead
Val Cofield, Senior Director and Task Force Three Lead
Cory Simpson, Senior Director and Directorate Four Lead
Benjamin Jensen, Senior Research Director and Lead Writer

WHITE PAPER LEAD WRITER
Robert Morgus, Director for Research and Analysis

FULL TIME STAFF
Laura Bate, Director for Cyber Engagement
Tatyana Bolton, Policy Director
Gregory Buck, Deputy Chief of Staff
Madison Creery, Cyber Strategy and Policy Analyst
Matthew Ferren, Cyber Strategy and Policy Analyst
Chris Forshey, Facility Security Officer
Karrie Jefferson, Director for Cyber Engagement
Ainsley Katz, Cyber Strategy and Policy Analyst
Alison King, Strategic Communications and Congressional Advisor
Sang Lee, Director for Cyber Engagement
Diane Pinto, Cyber Strategy and Policy Analyst
Brandon Valeriano, Senior Advisor

LEGAL ADVISORS
Stefan Wolfe, General Counsel
Corey Bradley, Deputy General Counsel
Cody Cheek, Legal Advisor
David Simon, Chief Counsel for Cybersecurity and National Security

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

The executive branch Commissioners contributed superb assessments, insights, and recommendations to the report and actively participated in the Commission's deliberations, but, in accordance with executive branch legal guidance, abstained from its final approval.


U.S. CYBERSPACE SOLARIUM COMMISSION