Congress of the United States
Washington, DC 20515

The Honorable Patrick Leahy
Chairman
Senate Committee on Appropriations
S-128, The Capitol
Washington, DC 20510

The Honorable Richard Shelby
Vice Chairman
Senate Committee on Appropriations
S-128, The Capitol
Washington, DC 20510

April 28, 2021

Dear Chairman Leahy and Vice Chairman Shelby:

On March 11, 2020, the Cyberspace Solarium Commission[1] published its recommendations for defending the United States in cyberspace. These recommendations served as the basis of 27 provisions that passed into law in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA). We are seeking your support for the funding recommendations below, which result both from these newly authorized activities and from Commission recommendations to strengthen efforts that are already authorized.

The Cyberspace Solarium Commission was established by the National Defense Authorization Act for Fiscal Year 2019 as a bipartisan, intergovernmental, and public-private body charged with evaluating approaches to defending the United States in cyberspace and driving consensus toward a comprehensive cyber strategy. The Commission was composed of 14 cyber experts, private-sector leaders, Members of Congress, and senior officials from the executive branch. The resulting report and subsequent white papers—which addressed the information and communications technology supply chain, the cybersecurity workforce, and lessons learned from the COVID-19 pandemic—include legislative, executive, and private sector solutions that will improve the United States' footing in cyberspace.

We ask that you support the following requests for increasing resources to existing and newly authorized programs that align with the Commission's work. For each request, the corresponding Commission recommendation is referenced in *italics*.

Commerce, Justice, Science, and Related Agencies

- With more than 37,000 open cybersecurity jobs, the public sector suffers from a significant shortage in its cyber workforce. Upon entering government, cybersecurity personnel must also have rewarding career paths and the education and training opportunities necessary to keep their skills relevant and up to date within a rapidly changing field. The CyberCorps®: Scholarship for Service (SFS) program, managed by the National Science Foundation in conjunction with the Department of Homeland Security and the Office of Personnel Management, awards scholarships to university students studying cybersecurity and, in return, requires the recipients to work for a federal, state, local, or tribal government organization in a position related to cybersecurity, or for a SFS school, upon graduation. **We recommend funding for the CyberCorps® program be set at $80 million in Fiscal Year 2022**, $20 million above the amount specified in the Joint Explanatory Statement to the Consolidated Appropriations Act for Fiscal Year 2021. Additional

[1] https://www.solarium.gov/

funding will allow for approximately 286 more scholarships to be awarded. **In addition, we request the following report language:**

"*CyberCorps®: Scholarship for Service*.—The Committee recommends not less than $80,000,000 for the CyberCorps®: Scholarship for Service program to increase the number of scholarships available to students. The National Science Foundation is encouraged to use the additional funding to increase the number of scholarships awarded at participating institutions and to increase the number of institutions that receive grants to participate in the program." *(Recommendation 1.5)*

- **Five of the Commission's recommendations impact the National Institute of Standards and Technology (NIST)**, reflecting the significance of this agency's work in promoting a secure cyberspace:

  1) Through its leadership, coordination, and participation in standards development, NIST plays a critical role in national and international standards development organizations. These organizations are pivotal in determining the future development of cyberspace, and participation in and contributions to these bodies are vital to American economic and security interests. In order to participate most effectively, NIST needs depth of technical expertise, understanding of the affected industries, knowledge of the standards organizations, and active and consistent participation in these bodies. *(Recommendation 2.1.2)*

  2) Among its core cybersecurity and privacy activities, NIST maintains the National Vulnerabilities Database, establishes review processes and standards for new cryptographic approaches, provides critical tools to advance software security nationwide, and offers frameworks for risk management and privacy. Because the need for these core functions is constantly growing as digital connectivity expands, NIST requires additional resources to continue to provide these core services. Meanwhile, new developments and evolving technologies have necessitated drastically scaling up existing projects, for example, in Internet infrastructure and Internet of Things (IoT) standards development. *(Recommendation 4.1.2)*

  3) Section 9401 of the FY21 NDAA authorized a program for regional cybersecurity workforce development programs administered by the National Initiative for Cybersecurity Education within NIST. The regional alliances and multi-stakeholder partnerships authorized in the legislation require a series of cooperative agreements with local partners, which may include funding. This mandate, and others implemented in Sections 9401 and 9402 of the FY21 NDAA on the cybersecurity workforce, require funding to enable implementation.[2] *(Recommendation 1.5)*

  4) Consumers lack the information needed to make security-conscious choices when selecting a cloud service provider. In collaboration with the Cybersecurity and Infrastructure Security Agency, NIST has the authorities needed to begin work towards a secure cloud certification with an increase in appropriated funding. *(Recommendation 4.5)*

  5) NIST most recently issued guidance on vulnerability patching implementation in 2013 in Special Publication 800-40. Given the pace of change in the cyber domain—and the fact that

[2] The Congressional Budget Office estimated costs for this program, originally introduced in 2019 as part of S. 2775, at $15 million during the program's first year. See: Congressional Budget Office, Budget Estimate for *S. 2775, HACKED Act of 2019* (Washington, DC, 31 January 2020), https://www.cbo.gov/system/files/2020-01/s2775.pdf

unpatched systems remain a major point of entry for malicious cyber actors—the guidance is due to be updated. *(Recommendation 4.2.1)*

To facilitate hiring scientists, engineers, and subject matter experts who can meet the increasing demands across multiple emerging technologies and to provide necessary support for those added positions, **we recommend appropriating $142.375 million for Cybersecurity and Privacy within the Scientific and Technical Research and Services account at NIST**, an increase of $64.875 million over the amount specified in the Joint Explanatory Statement to the Consolidated Appropriations Act for Fiscal Year 2021. **We further recommend the following report language:**

"*Cybersecurity and Privacy Standards.*—The Committee recommends, of funds allocated to Cybersecurity and Privacy within the National Institute of Standards and Technology, increases to the existing budget of not less than the specified amounts in the following areas for purposes including increasing personnel and contracting resources: $2,500,000 for vulnerability management, $2,500,000 for cryptography programs, $10,000,000 for privacy programs, $10,000,000 for identity and access management, $10,000,000 for software security, $3,000,000 for infrastructure with a particular focus on Domain Name System and Border Gateway Protocol security, $3,000,000 for the National Initiative for Cybersecurity Education with a particular focus on expanding workforce requirements authorized in Section 9401 and 9402 of the Fiscal Year 2021 National Defense Authorization Act, and $8,000,000 for Internet of Things security."

"*Cybersecurity Education Regional Alliances.*—The Committee strongly supports the amendments made to the Cybersecurity Enhancement Act of 2014 as part of the Fiscal Year 2021 National Defense Authorization Act, particularly with respect to regional alliances and multi-stakeholder partnerships. Therefore, the Committee recommends that not less than $12,000,000 of the funds made available for National Institute of Standards and Technology Cybersecurity and Privacy efforts be used for activities under section 401(f) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451), as amended."

"Cloud Security Certification.—The Committee encourages the development of a secure cloud certification that would provide information that consumers, including those in the public sector, need to make security-conscious choices when selecting a cloud service provider. The certification should account for and consolidate existing standards and certifications, including the NIST SP 800-37 and SP 800-53 controls that FedRAMP relies on, as well as existing private sector standards and certifications such as SOC 1 and SOC 2. Accordingly, the Committee recommends that not less than $3,875,000 be used to begin work towards developing a secure cloud certification."

"*Vulnerability Patching Guidance.*—The Committee notes that NIST last updated Special Publication 800-40, 'Guide to Enterprise Patch Management Technologies,' in 2013. Given the importance of timely patching to organizations maintaining a robust cybersecurity posture, no later than 120 days after the enactment of this Act, the National Institute of Standards and Technology is directed to report to the Committee about its plans to revise and update the Special Publication."

- There are currently 10 **FBI Cyber Assistant Legal Attaché** (ALATs) working in various U.S. missions around the world to facilitate intelligence sharing and help coordinate joint cyber operations. The Commission strongly believes in the effectiveness of these personnel and supports increased funding to allow more of them to be positioned at embassies of interest. In its 2020 report, the Commission recommended an additional 12 Cyber ALAT positions. Six additional positions were funded through the Consolidated Appropriations Act for Fiscal Year 2021; thus, we recommend an additional six. Accordingly**, we recommend that funding for the ALAT program be set at $17.6 million**, which would support 22 Cyber ALATs, **and the following report language:**

  "*Cyber Assistant Legal Attachés.*—The Committee strongly supports the FBI's Cyber Assistant Legal Attaché (ALAT) program, which facilitates intelligence sharing and helps coordinate joint law enforcement investigations. Eliminating safe havens for cyber criminals is a key priority, and international cooperation is essential to holding bad actors accountable. The Committee therefore recommends that not less than $17,600,000 in funding for the Cyber ALAT program, which will support 22 Cyber ALATs stationed at missions of key partners." *(Recommendation 2.1.4)*

- In order to support the creation and maintenance of federal programs designed to better recruit, develop, and retain cyber talent, policymakers need accurate, up-to-date data. In particular, more **research on the current state of the cyber workforce**, paths to entry, and demographics can help ensure that federal hiring programs progress in innovating recruitment, diversifying the workforce, and retaining top talent. Much of this research can be done using existing authorizations for the National Center for Science and Engineering Statistics (NCSES), which is tasked with providing statistical data on the U.S. science and engineering enterprise. To enable data-driven policy approaches to bolstering cybersecurity education, **we recommend an increase in appropriations for the NCSES of $1.25 million and the following report language:**

  "*Cybersecurity Workforce*.—The Committee recommends an increase for the National Center for Science and Engineering Statistics (NCSES) of $1,250,000 to undertake a study to identify, compile, and analyze existing nationwide data and conduct survey research as necessary to better understand the national cyber workforce. Noting the already low ratio of personnel to budget at NCSES relative to other federal statistical agencies, the Committee encourages expenditure of appropriated funds to support additional personnel, which may include statisticians, economists, research scientists, and other statistical and support staff as needed, to ensure adequate staffing for this research." *(Recommendation 1.5)*

- Across a wide range of issues, the increasing prevalence of disinformation spread online continues to undermine public confidence in critical institutions and the effectiveness of public messaging during times of crisis. Researchers, civil society organizations, and other nongovernmental organizations are already working to better understand and counter these threats. **We recommend that an increase of $3 million be appropriated to support the Department of Justice's Office of Justice Programs in providing grants to these organizations and the following report language:**

  "*Disinformation Research Grants.*—Of the funding appropriated for the Office of Justice Programs, not less than $3,000,000 will be used for research grants to nonprofit organizations seeking to identify, expose, and explain malign foreign influence campaigns to the American

public. Grants may be administered by a component of the Office of Justice Programs. The Committee encourages the administering office to work in consultation with the Department of Homeland Security and the National Science Foundation." *(Lessons from the Pandemic White Paper Recommendation 1.4)*

- The international telecommunications market is currently watching the race to develop **Fifth Generation (5G) technology**. However, maintaining competitiveness in the market for future generations of telecommunications technology will rely heavily on current investment in research and development in both the technologies themselves and the radio frequency spectrum management needed to enable next generation communications use. To support this investment in innovation, **we recommend an increase of $5 million over the Fiscal Year 2021 enacted levels for Advanced Communications Research at the National Telecommunications and Information Administration and the following report language:**

  "*Next Generation Communications Research*.—The Committee provides an increase of $5,000,000 for Advanced Communications Research at the Institute for Telecommunication Sciences to expand research and development in radio frequency spectrum management to allow next generation communications use and to ensure that 5G networks and the broader telecommunications supply chain are secure, including through vendor diversity." *(Supply Chain White Paper Recommendation 3.1)*

- A comprehensive understanding of cyber threats requires extensive **identification and tracking of foreign adversaries operating domestically**, generally accomplished through intelligence gathering; evidence collection; technical and human operations; and the cooperation of victims and third-party providers. The Federal Bureau of Investigation's (FBI) cyber mission—synthesized through the multiagency National Cyber Investigative Joint Task Force (NCIJTF) and a nationwide network of field offices and Cyber Task Forces—has a unique dual responsibility: To gather and leverage intelligence in order to prevent harm to national security and to enforce federal laws as the nation's primary federal law enforcement agency. Both roles are essential to investigating and countering cyber threats to the nation and are critical to whole-of-government campaigns supporting layered cyber deterrence, the strategic framework agreed upon by the Commission. To ensure that the FBI is properly resourced to carry out its cyber mission and perform attribution and also to strengthen whole-of-government counter-threat campaigns and enable other agency missions in support of national strategic objectives through NCIJTF, **we recommend funding FBI Cyber at a level of no less than $126.8 million**, $28.5 million above the Fiscal Year 2020 level, and $17 million above the Fiscal Year 2021 request, **and the following report language:**

  "*Cyber Threat Response.*—The Committee strongly supports the Bureau's activities in furtherance of its role as the lead agency for threat response pursuant to Presidential Policy Directive 41. As such, the funding recommendation includes an increase of $17,000,000 million over the Fiscal Year 2021 request for the National Cyber Investigative Joint Task Force. The FBI is expected to use additional National Cyber Investigative Joint Task Force funding to increase personnel available to support information sharing for cyber threat investigations." *(Recommendation 1.4.2)*

Defense

- Investing in the efforts of our international partners and allies to strengthen their cyber defenses improves the United States' ability to shape the behavior of other actors in cyberspace and pursue collective security in cyberspace with partners and allies. The **Defense Security Cooperation Agency**, through Regional Centers for Security Studies and the Institute for Security Governance, is a key implementer of institutional capacity-building programs. The Regional Centers for Security Studies provide courses and training to partner nations on cybersecurity and cyber defense, and the administration specifically referenced the George C. Marshall European Center for Security Studies as a provider of training on cyber incident attribution and cyber norms in response to harmful foreign activities of the Russian government.[3] The Defense Security Cooperation Agency also identified cybersecurity as a priority area for the Institute for Security Governance in Fiscal Year 2021. **Accordingly, we recommend the following report language:** (*Recommendation 2.1.3)*

  "*Regional Centers for Security Studies*.—Of the funds appropriated to the Regional Centers at the Defense Security Cooperation Agency, not less than $6,000,000 shall support efforts conducted by Regional Centers for Security Studies to build cyber capacity, cooperation, and interoperability with international partners and allies. In particular, the Committee strongly supports the administration's recent commitment to provide training for foreign policymakers and diplomats on the policy and technical aspects of public attribution and on the applicability of international law in cyberspace offered at the George C. Marshall European Center for Security Studies."

  "*Institute for Security Governance (ISG).*—Of funds appropriated to the Security Cooperation Act at the Defense Security Cooperation Agency, not less than $10,000,000 shall support the ISG's efforts as the primary implementer of Department of Defense institutional capacity-building programs and the ISG's focus on the priority area of cybersecurity."

- To counter cyber-enabled information operations, Americans must have the **digital literacy tools needed to evaluate the trustworthiness of information** spread on online platforms. Furthermore, because the intent of so many cyber-enabled information operations is to cause Americans to distrust or lose faith in the institutions of democracy, digital literacy should be coupled with civics education explaining what democracy is, how individuals can hold their leadership accountable, and why democracy must be nurtured and protected. The Commission supports efforts to develop robust civics education curricula that results in meaningful improvements in media literacy. In particular, **we support the research reauthorized in Section 234 of the National Defense Authorization Act for Fiscal Year 2020 and recommend an increase of $10 million in funding for the National Defense Education Program—program element number 0601120D8Z—to support the pilot program on enhanced civics education in Fiscal Year 2022.** *(Recommendation 3.5)*

[3] FACT SHEET: "Imposing Costs for Harmful Foreign Activities by the Russian Government" https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

- Section 5323 of the National Defense Authorization Act for Fiscal Year 2020 established the **Social Media Data and Threat Analysis Center** under the direction of the Director of National Intelligence. The legislation authorized appropriations of up to $30 million available for use in establishing the Center in Fiscal Years 2020 and 2021. To further the work of this important initiative in combating foreign influence through social media, **we recommend the following report language:**

  "*Social Media Data and Threat Analysis Center.*—The Committee notes with interest the announcement of the creation of the Foreign Malign Influence Center; however, it is unclear how the new center will work with the Social Media Data and Threat Analysis Center required by section 5323 of the National Defense Authorization Act for Fiscal Year 2020. Not later than 180 days after the enactment of this Act, the Director of National Intelligence is directed to submit a report to the congressional defense committees describing progress on establishing the Social Media Data and Threat Analysis Center and plans to integrate – and avoid duplication of – its work with the Foreign Malign Influence Center." *(Lessons from the Pandemic White Paper Recommendation 1.4.1)*

- Several of the Commission's recommendations center on **cybersecurity challenges related to emerging technologies**. Recent developments with 5G wireless technology have demonstrated the significant vulnerabilities that can arise, both domestically and internationally, without trusted suppliers. Emerging technologies such as artificial intelligence and quantum information science pose both opportunities and risks, and we need federal investment in basic and early stage applied research to better understand those risks, as well as to ensure the United States is poised to capitalize on those opportunities. Within the Department of Defense, the Defense Advanced Research Projects Agency has a long legacy of conducting exactly this kind of research, including on the precursor technologies to the Internet itself. **We therefore request $50 million in funding for Foundational Artificial Intelligence Science, an increase of $9 million above the Fiscal Year 2021 appropriated level, and $30 million for Alternative Computing, an increase of $6.087 million above the Fiscal Year 2021 appropriated level**. Both initiatives are part of program element 0601101E, project CCS-02. *(Recommendation 4.6.2)*

Financial Services and General Government

- The **National Cyber Director**, supported by the Office of the National Cyber Director, serves as the President's primary advisor for cyber and emerging technology issues; the lead for national-level coordination of U.S. cyber strategy and policy; and the chief U.S. representative and spokesperson on all cybersecurity-related issues. **Based on Section 1752 of the FY21 NDAA, which establishes the position and Office of the National Cyber Director, we recommend $50 million in funding, $25 million of which should remain available until September 30, 2023,** to support the Senate-confirmed position, office, and a staff of 25 non-reimbursable detailees and 50 employees. **We also recommend the following bill language:** *(Recommendation 1.3)*

  "OFFICE OF THE NATIONAL CYBER DIRECTOR SALARY AND EXPENSES - For necessary expenses of the Office of the National Cyber Director, including the hire of passenger motor vehicles; for the employment of experts and consultants as authorized by Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021; and

for participation in joint projects or in the provision of services on matters of mutual interest with nonprofit, research, or public organizations or agencies, with or without reimbursement, $50,000,000, of which not to exceed $50,000 shall be available for official reception and representation expenses; Provided, that $25,000,000 shall remain available until September 30, 2023: Provided further, that the Office is authorized to accept, hold, administer, and utilize gifts, both real and personal, public and private, without fiscal year limitation, for the purpose of aiding or facilitating the work of the Office."

- **Cybersecurity threats to our elections** are a growing concern in the United States. The Election Assistance Commission's (EAC) mission is to help election officials improve the administration of elections and improve voter participation, yet it suffers from chronic funding and personnel shortages that prevent it from accomplishing those goals. Increased funding will allow it to assist states and localities in defense of the digital election infrastructure that underpins federal elections and to ensure the widest use of voter-verifiable, auditable, and paper-based voting systems. **We recommend an appropriation of $24 million for the EAC in Fiscal Year 2022**, which would represent an increase of $7 million above the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021. *(Recommendation 3.4)*

- As codified in the FY21 NDAA, **Sector Risk Management Agencies (SRMAs)** manage much of the day-to-day engagement between the federal government and private-sector entities within a given critical infrastructure sector. National resilience requires that each of these agencies be able to identify, assess, and support the private sector in managing risks, which can manifest in both the physical and cyber domains and across sectors. We recognize that the Department of Treasury has a mature plan for managing risk within the Financial Services sector, but it lacks appropriate funding. **We therefore recommend that the Office of Cybersecurity and Critical Infrastructure Protection receive $25 million, an increase of $11.8 million over the amount specified in the Fiscal Year 2021 request,** to increase funding available for additional personnel in order to support communication and coordination with the financial services sector. *(Recommendation 3.1)*

- The Commission supports strengthening the capacity of the **Committee on Foreign Investment in the United States (CFIUS)**. Specifically, the Commission raised concerns about the adequacy of CFIUS reviews of bankruptcy buyouts and restructuring, as well as early-stage venture capital and private equity investment in companies of interest. Federal bankruptcy judges are a key component to this recommendation. **Therefore, we recommend the following report language:**

  "*Bankruptcy, Investment, and National Security.*—The Committee recognizes the importance of national security considerations in reviewing bankruptcy and investment transactions, and therefore encourages the Federal Judicial Center, acting through the activities of the Education and Training program, to support the education of bankruptcy judges on the Committee on Foreign Investment in the United States process and how bankruptcy court decisions impact the process and national security. To that end, not later than 180 days after the enactment of this Act, the Center is directed to report to the Committee its plans for incorporating national security considerations into bankruptcy judge educational activities." *(Recommendation 4.6.3)*

- Just as the security features of consumer electronics vary, so do the **security features of the industrial control systems** that digitally oversee critical infrastructure nationwide. A major

challenge in improving the security of these networks stems from the lack of information available to owners and operators as they purchase new devices to introduce to their networks. The establishment of a National Cybersecurity Certification and Labeling Authority, as was recommended by the Commission, would make it significantly easier for critical infrastructure owners and operators to purchase secure information and communications technologies. **We recommend the following report language:**

"*Cybersecurity Certification and Labeling.*—The Committee encourages the Federal Communications Commission's Office of Engineering and Technology, Laboratory Division to begin work in assessing existing cybersecurity certifications pertinent to critical infrastructure and developing further informational and technological resources, as needed, to inform consumer and critical infrastructure owner and operator purchasing decisions for secure information and communications technologies." *(Recommendation 4.1)*

Homeland Security

- The **Cybersecurity and Infrastructure Security Agency (CISA)** is intended to be a keystone of national cybersecurity efforts, and the FY21 NDAA granted additional authorities to expand and strengthen the agency. Accordingly, we offer the following recommendations:

1) As codified in Section 9002 of the FY21 NDAA, Sector Risk Management Agencies (SRMAs) manage much of the day-to-day engagement between the federal government and private-sector entities within a given critical infrastructure sector, and CISA is responsible for eight of these sectors. Additionally, CISA provides overall coordination of the sector partnership model, which requires CISA to work closely with all SRMAs across the interagency. The increased responsibilities placed on SRMAs in the FY21 NDAA necessitates additional resources in furtherance of these obligations and creates new opportunities for CISA to advance resilience nationwide. *(Recommendation 3.1)*
2) The National Risk Management Center (NRMC) partners with the critical infrastructure community to understand and manage risk to National Critical Functions. Among its core responsibilities, NRMC performs risk assessments, modeling, and data management and visualization. In order to continue to inform risk management decisions, NRMC must grow. This will require investments in personnel, office space, and tools central to the NRMC mission. *(Recommendation 3.1)*
3) Section 9603 of the FY21 NDAA authorized the development of a Continuity of the Economy Plan, a plan to maintain and restore the economy of the United States in response to a significant event. This effort will require personnel and administrative support services, including office space and classified and unclassified communications. *(Recommendation 3.2)*
4) While Congress has recently significantly increased support for cybersecurity capacity on federal networks, CISA's mission relies on its ability to serve all critical infrastructure regardless of size or proximity to the D.C. area. Small and medium-sized enterprises and state, local, tribal, and territorial governments are not resourced enough to meet the scale and sophistication of the intrusions they face. To help bridge this gap, the Commission recommends expanding CISA's services and technical assistance capabilities by increasing the capacity of its Hunt and Incident Response Teams and designating a subset of the teams for non-Federal activities. *(Recommendation 1.4)*
5) Recent appropriations have provided additional support for provision of cybersecurity services

to the federal government, but similar needs exist beyond the federal space. In particular, CISA is responsible for providing assessments to identify and eliminate cyber vulnerabilities. An increase in funding to support additional positions in CISA will allow the agency to expand provision of these assessments and facilitate information sharing. *(Recommendation 1.4)*

6) CISA's Cybersecurity Advisors (CSAs) operate via CISA's existing network of ten regional offices to bring critical cybersecurity expertise to underserved geographic areas and stakeholder bases. Section 1717 of the FY21 NDAA authorized the appointment of a cybersecurity coordinator for each state, which expanded the program's geographic coverage. However, in locations that are home to a high density to critical infrastructure, a single coordinator will be insufficient to meet the requirements to provide a more mature risk analysis and measurements capability outside of the federal network and provide an increased ability to support special projects and national level events. *(Recommendation 1.4)*

7) Section 1731 of the FY21 NDAA authorized planning to begin for an Integrated Cyber Center (ICC) within CISA to help the agency accomplish its mission of bolstering the resilience and security of American critical infrastructure. The ICC would draw on expanded capabilities across existing programs within CISA's Cybersecurity Division. Per that legislation, a report detailing the plan to create the ICC is due January 1, 2022, one year from the date of enactment of the FY21 NDAA. *(Recommendation 5.3)*

8) In order to truly operationalize cybersecurity collaboration with the private sector, the U.S. government must improve CISA's connectivity with other key cyber and cybersecurity centers and strengthen its ability to ensure that the systems, processes, and human element of collaboration and integration are fully brought to bear in support of the critical infrastructure cybersecurity and resilience mission. *(Recommendation 5.3)*

9) Section 1715 of the FY21 NDAA authorized the creation of a Joint Cyber Planning Office (JCPO) within CISA to coordinate cybersecurity planning and readiness across the federal government and between public and private sectors for significant cyber incidents and malicious cyber campaigns. Additional funding would allow the work of the JCPO to continue while accounting for increasing staff numbers as the office reaches full capacity. *(Recommendation 5.4)*

10) Section 1719 of the FY21 NDAA codified CISA's Cybersecurity Education Training Assistance Program, which supports cybersecurity curriculum development, "train-the-trainer" resources for elementary and secondary school teachers, and other classroom resources. Additional resources would expand the reach of the program in classrooms across the country. *(Recommendation 1.5.1)*

11) The United States has lacked a recurring, senior-level exercise that tests the resilience, response, and recovery of the United States to a significant cyber incident. Section 1744 of the FY21 NDAA authorized such an exercise. *(Recommendation 3.3.5)*

12) Voluntary threat detection programs are essential to building resilience of non-federal networks by improving knowledge of the cyber threats affecting U.S. critical infrastructure, but these programs have been hindered by a limited scale of deployment and insufficient coverage. Expanding programs, like the existing Cyber Sentry program, would enable more proactive identification and response to cyber incidents in critical infrastructure by deploying additional sensors at the point where industrial control systems connect to information technology networks. This is separate and apart from efforts carried out within the Department of Energy. *(Recommendation 5.2.1)*

13) Insurance can incentivize organizational cybersecurity behavior, but the market for cyber insurance is nascent and limited by a lack of quality datasets and models needed to understand, appropriately price, and mitigate cyber risk. A public-private working group established within

CISA can help develop frameworks and models for understanding and pricing cyber risk and identify areas of interest for pooling public and private sector data that can inform better, more accurate risk models. *(Recommendation 4.4.1)*

These thirteen priorities represent our recommendations as commissioners with the Cyberspace Solarium Commission, which are intended to be considered alongside, not in place of, increases to base funding due to normal maturation at the agency and other priorities represented in the President's budget request.[4]

To facilitate these activities, **we recommend an increase in appropriations of $142.229 million for the following accounts at the Cybersecurity and Infrastructure Security Agency (all specified at PPA Level II): $64.604 million for Cyber Operations, $8 million for Integrated Operations, $29.279 million for Risk Management Operations, $2 million for Infrastructure Assessments and Security, and $38.346 million for Stakeholder Engagement and Requirements.**

Figure 1: Recommended Increases to CISA Budget by Account

		CISA Budget Item							
	Amounts in Millions as Increases to Consolidated Appropriations Act for FY21	Cyber/Cyber Ops/ Threat Hunting	Cyber/Cyber Ops/ Vuln Management	Cyber/Cyber Ops/ Capacity Building	Cyber/Cyber Ops/ Op Planning and Coord	Infra. Security/Infra. Assessments & Security /CISA Exercises	Integrated Operations/ Regional Operations	Risk Managm't Ops/ Risk Managm't Ops	Stakeholder Engagement and Reqs/SE&R
Solarium Recommendation	1.4 - Non-Fed HIRT	$7							
	1.4 - Non-Fed Services		$10.022						
	1.4 - Cyber Security Advisors						$8		
	1.5.1 - CETAP			$2.15					
	3.1 - SRMA Managm't								$38.346
	3.1 - NRMC							$22.20	
	3.2 - Cont. of the Econ.							$7.079	
	3.3.5 - Sr. Level Exerc.					$2			
	5.2.1 - Threat Detection	$20		$6					
	5.3 - Communications Integration			$8	$3.45				
	5.4 - JCPO				$7.982				

[4] The Commission also supports additional funding for Federal Network Resilience efforts supported by supplemental appropriations earlier this year. While the $650 million provided as part of that effort will support many important initiatives, additional appropriations will be necessary to ensure enhanced monitoring is available across all Federal civilian agencies.

We further recommend the following report language:

"*Sector Risk Management Agencies.*—The Committee recognizes CISA is the Sector Risk Management Agency for the Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste sectors. Accordingly, not less than $56,000,000, which is an increase of $38,346,000 above the amount specified in the Joint Explanatory Statement accompanying the Consolidated Appropriations Act for Fiscal Year 2021, of the funds appropriated for the Stakeholder Engagement and Requirements account at CISA are to be used for activities carried out in furtherance of the authorities and added requirements established Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 for the management of these eight sectors. In order to better support coordination of Sector Risk Management Agencies across the federal government, the Committee urges CISA to consider personnel increases to support cultivation of sector-specific expertise within the agency, including and extending beyond the eight sectors for which CISA serves as the Sector Risk Management Agency. These increases may include temporary hires and advisory positions, additional full-time employees, and reimbursement for personnel on detail from other departments and agencies."

"National Critical Functions (NCFs) Analytic Capability.—The Committee provides an increase of $22,200,000 above the amount specified in the Joint Explanatory Statement to the Consolidated Appropriations Act for Fiscal Year 2021 to develop an agile analytic capability that can evaluate evolving strategic technology risks for NCF assets over a 5- to 20-year timespan. The National Risk Management Center is directed to brief the Committee not later than 60 days after the date of enactment of this Act on a plan of action and milestones for bringing this capability online, including a budget and hiring plan."

"*Continuity of the Economy Plan.*—Not less than $7,079,000 of the funds appropriated for the to the National Risk Management Center through the Risk Management Operations account at the Cybersecurity and Infrastructure Security Agency are to be used for activities carried out in furtherance of Section 9603 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 to develop a Continuity of the Economy Plan."

"Hunt and Incident Response Teams (HIRTs).—In order to support incident response and threat hunting capabilities on non-federal networks at the request of state, local, tribal, and territorial governments and critical infrastructure owners and operators, the Committee provides an increase of $7,000,000 above the amount specified in the Joint Explanatory Statement to the Consolidated Appropriations Act for Fiscal Year 2021 for Threat Hunting within the Cyber Operations budget. Funding will support a new non-Federal HIRT to respond to requests on non-Federal networks, including state, local, tribal, and territorial governments and other critical infrastructure owners and operators."

"Vulnerability Management Infrastructure.—The Committee recognizes that as the number of networked devices across cyberspace increases exponentially, so does the number of identified and reported vulnerabilities in the software and hardware that operates critical infrastructure globally. The Committee provides an increase of $10,022,000 above the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021 for the underlying infrastructure that enables better identification, analysis, and publication of known vulnerabilities and common

attack patterns, including through the National Vulnerability Database, and to expand the coordinated responsible disclosure of vulnerabilities."

"*Cybersecurity Advisors (CSAs)*.—The agreement includes an increase of $8,000,000 to increase the number of CSAs in the ten CISA regional offices. These advisors will be in addition to the state cybersecurity coordinators established in furtherance of Section 1717 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, in order to supplement regional capability."

"*Integrated Cyber Center.*—In furtherance of Section 1731 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Committee looks forward to reviewing the report due on January 1, 2022, on the potential for better coordination of Federal cybersecurity efforts at an integrated cybersecurity center within the Cybersecurity and Infrastructure Security Agency."

"*Cybersecurity Communication and Center Integration.*—The Committee recommends an increase in funding of not less than $11,450,000 to support functions including receiving, analyzing, integrating, and providing information related to cyber threat indicators, defensive measures, cybersecurity risks, supply chain risks, incidents, analysis, and warnings, and providing technical assistance and risk management support to Federal and non-Federal entities. Funding shall be used to meet the facilities and staffing requirements needed to perform the functions of the national cybersecurity and communications integration center."

"Joint Cyber Planning Office.—In furtherance of Subtitle A of Title XXII of the Homeland Security Act of 2002 as amended by Section 1715 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, not less than $18,550,000, an increase of $7,982,000 over the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021, of funds appropriated for Operational Planning and Coordination within the Cyber Operations budget at the Cybersecurity and Infrastructure Security Agency will be used to fund the hiring of personnel, reimbursement of detailees from other federal agencies, and such equipment as is necessary for the operations of the Joint Cyber Planning Office."

"*Cybersecurity Education Training Assistance Program.*—Not less than $6,450,000, an increase of $2,150,000 over the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021, of funds appropriated for Capacity Building within the Cyber Operations budget at the Cybersecurity and Infrastructure Security Agency will be used for activities carried out in furtherance of Section 2202(c) of the Homeland Security Act of 2002 as amended by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021."

"*Biennial Senior Leader Cyber Exercise.*—In furtherance of Section 1744 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, not less than $2,000,000 of funds appropriated to the Cybersecurity and Infrastructure Security Agency Exercises account within the Agency's Infrastructure Assessments and Security account will be used for the planning and execution of a biennial, national-level cyber tabletop exercise. These exercises shall involve senior leaders from the executive branch, Congress, state governments, the private sector, and international partners."

"*Cybersecurity Insurance Working Group.*—The Committee supports the creation of a public-private working group housed within CISA to help develop frameworks and models for understanding and pricing cyber risk and to identify areas of interest for pooling public and private sector data that can inform better, more accurate risk models."

"*Voluntary Threat Detection Programs.*— The Committee recommends an increase of not less than $20,000,000 over the amount specified in the Joint Explanatory Statement to the Consolidated Appropriations Act for Fiscal Year 2021 for Threat Hunting in the Cyber Operations account at the Cybersecurity and Infrastructure Security Agency and an increase of $6,000,000 over the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021 for Capacity Building in the Cyber Operations account at the Cybersecurity and Infrastructure Security Agency to be used to expand ongoing programs, including CyberSentry, for voluntary threat detection in critical infrastructure. Funds will be used to support work with critical infrastructure providers enabling the voluntary placement of sensors at the boundary between operational technology and information technology systems. Expenditures may include increases in personnel support to programs, the procurement and installation of sensors, system integration support, and contractor support for coordinating with participating organizations."

- **Speed is critically important when responding to an unfolding or anticipated cyber incident**. In the event of such an incident, prior planning can mitigate the harm done by delays needed to ensure adequate funding in the right account. A Cybersecurity Response and Recovery Fund (CRRF) would ensure that cybersecurity leaders have funding at the ready in order to ensure national capacity to respond to and recover from a significant cyber incident with the requisite speed and agility. To ensure adequate funding availability to provide incident response in the event of a recent, unfolding, or anticipated significant cyber event, **we support the President's budget request of $20 million for a CRRF within the Department of Homeland Security**, and the following report language:

  "*Cybersecurity Response and Recovery Fund*.—The Committee strongly supports the establishment of a Cybersecurity Response and Recovery Fund as described in the request. Funds shall be used to augment or scale up government asset response efforts, including through reimbursement to federal agencies and activation of standby contracts, in support of public and private critical infrastructure if a significant cyber incident has occurred or if there is a near-term risk of a significant cyber incident. Funded asset response activities may include furnishing technical and advisory assistance to entities affected by a cyber incident to protect their assets, mitigate vulnerabilities, and reduce the related impacts; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery." *(Recommendation 3.3)*

Labor, Health and Human Services, Education, and Related Agencies

- To counter cyber-enabled information operations, Americans must have the digital literacy tools needed to evaluate the trustworthiness of information spread on online platforms. Furthermore, because the intent of so many cyber-enabled information operations is to cause Americans to distrust or lose faith in the institutions of democracy, digital literacy should be coupled with

civics education explaining what democracy is, how individuals can hold their leadership accountable, and why democracy must be nurtured and protected. **To increase the quality of civics education, we recommend establishing a National Education Research and Development Center within the Institute for Education Sciences with $10,000,000 in funding** dedicated to improving resilience to misinformation by funding research on improving media literacy, digital civic engagement, and academic outcomes in civics and history. **We further support the following report language:**

"*Improving Civics Education.*—The Committee applauds the work of the Institute for Education Sciences (IES) and their efforts to identify which pedagogical methods and curricula improve learning outcomes. Civics education is a topic of growing importance, but many programs do not incorporate practices for civic engagement in the digital environment. Students must understand concepts such as media literacy, the role of cognitive bias in powering disinformation campaigns, responsible content sharing, and the prevalence of malicious online influence in order to effectively participate in our democracy and public discourse. Therefore, the Committee directs the Director of IES to establish a National Education Research and Development Center, within the National Center for Education Research, dedicated to improving young and adult learners' resilience to misinformation and disinformation. This center shall research which educational activities improve critical thinking, media literacy, and digital citizenship; enhance understanding of voting and other forms of political and civic engagement; increase awareness and interest in employment and careers in public service; improve understanding of United States law, history, and government; improve the ability of participants to collaborate and compromise with others to create safe, inclusive communities and solve local and global problems; expand awareness of foreign and domestic malign influence and the harm in spreading false information; and strengthen participants' ability to evaluate the perspective, accuracy, and validity of information. Of the funds appropriated for IES, not less than $10,000,000 shall be used for this purpose." (*Recommendation 3.5)*

Legislative Branch

- **Congress is in need of technical expertise to inform its members on cyber and technology policy issues**. Before it was dissolved in 1995, the Office of Technology Assessment (OTA) produced over 700 reports for both congressional and public consumption, ensuring the legislative branch was fully informed on technology related legislative issues. Other congressional efforts to build capacity in this area have not satisfactorily filled the gap left by its loss. **We recommend that the Committee provide $6 million in funding to reconstitute OTA** to provide unbiased expertise required to inform the legislative process on cutting-edge issues. *(Recommendation 1.2.1)*

State, Foreign Operations, and Related Programs

- **Investing in the efforts of our international partners and allies** to strengthen their cyber capabilities improves our own cybersecurity. It also creates an incentive for these countries to continue collaborating with the United States to shape behavior and impose consequences for malign activity in cyberspace. Current U.S. capacity-building efforts draw from a range of programs and funds. In order to allow the expansion of international cybersecurity capacity building across different geographic regions and for varied purposes we recommend the following increases, all relative to Fiscal Year 2021 enacted spending unless otherwise specified,

to five funds that support different aspects of international cybersecurity capacity building *(Recommendation 2.1.3)*:
1) **$20 million increase for the Economic Support Fund (ESF) for cyber capacity building**, bringing the total designated for cybersecurity capacity building within ESF to $27 million.
2) **$10 million increase for the Assistance for Europe, Eurasia, and Central Asia Fund for cyber capacity building**. Cyber capacity building efforts in this region would improve security in the region and cybersecurity globally by strengthening allies' and partners' capability to counter Russian influence and aggression.
3) **$7.5 million increase for the International Narcotics Control and Law Enforcement Fund** for countering cybercrime and intellectual property theft, bringing the total designated for countering cybercrime and intellectual property theft to $17.5 million. This recommended increase would support the development and expansion of projects designed to strengthen cooperation among law enforcement and other criminal justice sector professionals on cybercrime issues.
4) **$5 million increase for the Digital Connectivity and Cybersecurity Partnership** to support the partnership's focus on enhancing cybersecurity.
5) **$15 million increase for Foreign Military Financing** for bolstering allies' and partners' capability to provide for their own defense in cyberspace.

We further recommend the following report language:

"*International Cybersecurity Capacity Building.*—Of funding appropriated for the Economic Support Fund, not less than $27,000,000 will be used for international cybersecurity capacity building efforts that strengthen civilian cybersecurity through support to countries and organizations, including national and regional institutions. "

"*Building Cybersecurity in Eastern Europe.*—Of funding appropriated for the Assistance for Europe, Eurasia, and Central Asia Fund, not less than $10,000,000 will be used for international cybersecurity capacity-building efforts that may include a focus on strengthening collective commitments to security in cyberspace, combatting the coercive influence of Russian cyberattacks by strengthening incident response and remediation capabilities among the Visegrad 4 and Baltic nations, and providing resources and training to diplomats and policymakers on the applicability of international law in cyberspace and the policy and technical aspects of public attribution of cyber incidents.*"*

"*Countering International Cybercrime.*—Of funding appropriated for the International Narcotics Control and Law Enforcement Fund, not less than $17,500,000 will be used for capacity building efforts to counter cybercrime, which may include strengthening the ability of foreign policymakers to develop, revise, and implement national laws, policies, and procedures to address cybercrime and strengthening the ability of law enforcement to hold malign actors accountable.*"*

"*Digital Connectivity and Cybersecurity Partnership*.—The Committee recommends an increase of not less than $5,000,000 over the amount specified in the Consolidated Appropriations Act for Fiscal Year 2021. The Trade and Development Agency shall support international cybersecurity capacity building efforts that foster government-industry cooperation on cybersecurity, building cultures of cybersecurity within citizen populations, and strengthening capacity to deal with cybercrime."

"*Military Cybersecurity Capacity Building*.—Of funding appropriated for Foreign Military Financing, not less than $15,000,000 will be used for international cybersecurity capacity building efforts that strengthen the resilience and readiness of military cyber defenses and encourage regional cooperation against nation-state cyber threats like those emanating from Russia and China."

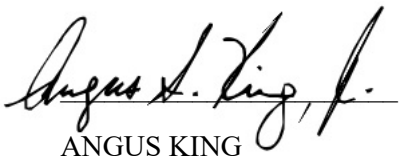
"*Capacity Building Administration.*—The Committee recognizes the growing importance of cybersecurity capacity building and the need for personnel experienced in cybersecurity issues to carry out the national cybersecurity strategy. Therefore the Committee recommends the Department expand efforts to hire experienced personnel to support cybersecurity capacity building."

- As countries with **less mature information communication technology (ICT) infrastructure race to advance their digital ecosystem, any donor nation offering support may be welcome**. China, in particular, often supports the development of ICT infrastructure abroad. However, not all donations of ICT infrastructure are created equally with respect to cybersecurity, which can inhibit the advancement of an open, interoperable, reliable, and secure global Internet. To enable countries to be discerning in their ICT infrastructure development projects, the Commission has recommended the development of a digital risk impact assessment. To allow the United States Agency for International Development to begin work on developing and implementing digital risk impact assessments for U.S. foreign assistance programs, **we recommend an increase of $5 million for the Bureau for Development, Democracy, and Innovation's Innovation, Technology, and Research hub**, and the following report language:

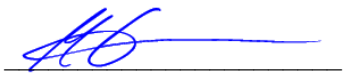
  "*Digital Risk Impact Assessments.*—Of amounts appropriated to the Bureau for Development Democracy and Innovation at the United States Agency for International Development through the Democracy Fund, not less than $5,000,000 will be used to develop tools and methods to aid in evaluating the risk incurred through information communication technology development projects." *(Supply Chain White Paper Recommendation 5.1)*

Thank you for your consideration of these requests and for your continued commitment to strengthening our nation's cybersecurity.

Sincerely,



ANGUS KING
U.S. Senator



MIKE GALLAGHER
Member of Congress

CC: Hon. Jeanne Shaheen
Hon. Jerry Moran
Hon. Jon Tester

Hon. Chris Van Hollen
Hon. Cindy Hyde-Smith
Hon. Chris Murphy
Hon. Shelley Moore Capito
Hon. Patty Murray
Hon. Roy Blunt
Hon. Jack Reed
Hon. Mike Braun
Hon. Christopher Coons
Hon. Lindsey Graham