April 3, 2020

The Honorable Richard Shelby
Chairman
Senate Committee on Appropriations
128 Russell
United States Senate
Washington, DC 20510

The Honorable Patrick Leahy
Vice Chairman
Senate Committee on Appropriations
128 Russell
United States Senate
Washington, DC 20510

Dear Chairman Shelby and Vice Chairman Leahy

On March 11, the Cyberspace Solarium Commission published its recommendations for defending the United States in cyberspace. We are seeking your support for the resulting funding recommendations outlined below that the Commission unanimously agreed to in its recent report.

The Cyberspace Solarium Commission was established by the 2019 National Defense Authorization Act 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 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 includes more than 75 actionable recommendations including legislative, executive, and private sector solutions that will improve the United States' footing in cyberspace.

Several of those recommendations involve appropriating resources to existing programs. We ask that you support the following requests for increasing resources to existing programs that were endorsed by the Commission. For each request, the corresponding Commission recommendation is referenced in *italics*.

Commerce, Justice, Science, and Related Agencies

- A comprehensive understanding of the cyber threat 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, **the Commission recommends funding FBI Cyber at a level of $126.8 million**, $28.5 million above the FY20 level, and $17 million above the FY21 request. (*Recommendation 1.4.2*)

- The federal government 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 with a rapidly changing field. The CyberCorps®: Scholarship for Service program, cosponsored by the National Science Foundation (NSF) and the Department of Homeland Security, awards scholarships to 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. **The Commission recommends funding for the CyberCorps® program be set at $75 million in FY21**, $20 million above the FY20 enacted level and $22 million above the FY21 request. (*Recommendation 1.5*)

- The ability to participate, contribute, and lead efforts in national and international Standards Development Organizations (SDOs) and Standards Setting Organizations (SSOs) are of vital economic and security interest to the nation. The National Institute of Science and Technology (NIST) through its leadership, coordination, and participation in standards development plays a critical role for the U.S. Government. In order to be most effective, NIST needs depth of technical expertise; understanding of the affected industries; knowledge of the standards organizations and active and consistent participation in these bodies. As the U.S. Government's body that identifies, harmonizes, and develops technology standards, guidelines, tools, and measurement capabilities, NIST is uniquely positioned to advance innovations in cybersecurity and technology security. NIST employs some of the country's leading experts in cyber and technologies, yet it lacks the resources necessary to meet the increasing demands on its staff. NIST requires additional resources in order to provide the number of scientists and engineers with the requisite expertise necessary to meet the increasing demands across multiple emerging technologies. NIST also requires increased funding to coordinate with interagency and private sector experts on participation at SDOs and SSOs. **The Commission therefore recommends providing $107.5 million for Cybersecurity and Privacy** within the Scientific and Technical Research and Services account, an increase of $30 million from FY20. (*Recommendations 2.1.2, 4.1.2*)

- There are currently 10 FBI Cyber Assistant Legal Attaches (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. The FY21 request includes funding for 6 additional Cyber ALATs. **The Commission recommends that funding for the ALAT program be set at $17.6 million**, which would support 22 Cyber ALATs, 6 above the request and 12 above the current level. (*Recommendation 2.1.4*)

Defense

- Several of the Commission's recommendations center on the cybersecurity challenges related to emerging technologies. Recent developments with Fifth Generation (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 and to ensure the United States is poised to capitalize on those opportunities. Within the Department of Defense, the Defense Advanced Research Projects Agency (DARPA) has a long legacy of conducting exactly this kind of research, including on the precursor technologies to the Internet itself. **The Commission therefore recommends $50 million in funding for Foundational Artificial Intelligence Science, an increase of $14.1 million above the FY21 request, and $30 million for Alternative Computing, an increase of $9.087 million above the FY21 request**. Both initiatives are part of program element 0601101E, project CCS-02. (*Recommendation 4.6.2*)

- 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 result in meaningful improvements in media literacy. In particular, **the Commission supports the research authorized in Section 234 of the FY20 National Defense Authorization Act and recommends $10 million in funding for the program in FY21**. (*Recommendation 3.5*)

- In order to monitor and support the implementation of the Commission recommendations, responsibility for this role must be designated to a specific actor. Extending the term of the Commission while constraining the staff to no more than three people would create the mandate and personnel needed to revise and iterate on legislative efforts at the behest of Congress, and monitor the implementation of report recommendations. **The Commission recommends an appropriation to the Department of Defense, Washington Headquarters Service not to exceed $1 million for this monitoring and implementation program in FY21.**

Financial Services and General Government

- 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. **The Commission recommends an appropriation of $20 million for the EAC in FY21**, which would represent an increase of $5 million above the FY20 level. (*Recommendation 3.4*)

- 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, the Commission recommends $26.4 million for the Federal Judicial Center, Education and Training program activity**, $4.4 million above

the FY20 enacted level, to support the education of bankruptcy judges on the CFIUS process and how bankruptcy court decisions impact the process and national security. (*Recommendation 4.6.3*)

- As defined in Presidential Policy Directive 21, Sector-Specific Agencies (SSAs) 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 domain and across sectors. The Commission recognizes that the Department of Treasury has a mature plan for managing risk within the Financial Services sector, but it lacks appropriate funding. **The Commission therefore recommends that the Office of Cybersecurity and Critical Infrastructure Protection receive $25 million**, an increase of $15.5 million over the FY20 enacted level and an increase of $11.8 million above the FY21 request. (*Recommendation 3.1*)

Homeland Security

- The Cybersecurity and Infrastructure Security Agency's (CISA) 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 in its ten regions by providing funding for one resident Hunt and Incident Response Team (HIRT) per region. Thus, **the Commission recommends a $40 million increase to CISA's Cyber Operations function** for ten HIRTs to ensure that one team is stationed at each of the ten regional CISA offices. (*Recommendation 1.4)*

- To fully implement the Cybersecurity and Infrastructure Security Act of 2018, which established CISA as an operational component agency under the Department of Homeland Security (DHS), we recommend providing additional funding for 'mission support' expenses. To be a fully operational agency within DHS, CISA must have sufficient resources to fund its own procurement, acquisition, human resources, and strategy, policy, and planning offices. **The Commission supports the President's budget request of $141,145,000 for CISA Operations and Support, Mission Support** up from the current FY20 enacted level of $84,677,000. (*Recommendation 1.4)*

- Preparedness planning leads to defined response mechanisms, public awareness, and improved response. In practice however, plans are thwarted by unforeseen challenges. Exercises build understanding of how complex systems will react in a time of disruption or crisis, building cohesion among disparate entities coordinating the response and promoting unity of effort that is crucial when catastrophes arise. To expand cross-sector cyber exercises, gaming, and simulations, **the Commission recommends $14 million, an increase of $7 million over the FY20 enacted level and $10 million over the FY21 request, for the National Infrastructure Simulation and Analysis Center** as part of CISA's Risk Management Operations program. (*Recommendation 3.3.4*)

- A safe and secure cyberspace depends on the trust and education of its users. A third of all data breaches still stem from a malign actor's success in persuading individuals to open phishing

emails, and cyber-enabled information operations are increasingly aimed at assaulting the societal trust that occurs outside of cyberspace. The Commission recommends funding public awareness campaigns to improve citizens' resiliency to these attacks. **The Commission recommends $5.5 million be appropriated for Cyber Education & Awareness** within CISA Cybersecurity Operations and Support. This will bring funding in line with FY14 levels. (*Recommendation 3.5*)

- As defined in Presidential Policy Directive 21, Sector-Specific Agencies (SSAs) 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 domain and across sectors. CISA is the SSA for the Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste sectors. **The Commission recommends the Committee provide $19.756 million for Sector Specific Agency Management** within CISA's Stakeholder Engagement and Requirements, an increase of $5 million above the FY21 request, for the management of these eight sectors. (*Recommendation 3.1*)

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. The Commission recommends funding efforts to develop tools and curricula to provide this education **and recommends $18 million be appropriated for American History and Civics National Activities** within the Innovation and Improvement account at the Department of Education, an increase of $15 million above the FY20 enacted level. (*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. **The Commission recommends 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*)

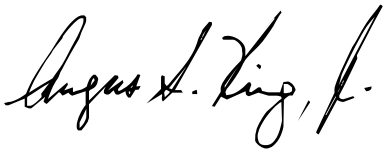
State, Foreign Operations, and Related Programs

- Investing in the efforts of our international partners and allies to build 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. **The Commission recommends the Committee provide an additional $10 million** for the Economic Support and Development Fund for cyber capacity building and

include report language requiring funding of cyber capacity building at a level at least $10 million higher than FY20. (*Recommendation 2.1.3*)

Thank you for your consideration of these requests.

Sincerely,



ANGUS S. KING, JR.
Co-Chairman
Cyberspace Solarium Commission

MIKE GALLAGHER
Co-Chairman
Cyberspace Solarium Commission