

Congress of the United States
Washington, DC 20515

March 22, 2022

The Honorable Charles E. Schumer
Majority Leader
United States Senate
322 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
317 Russell Senate Office Building
Washington, D.C. 20510

Dear Leader Schumer and Leader McConnell:

As co-chairs of the Cyberspace Solarium Commission, we are eager to see Congress address much-needed cybersecurity shortfalls and improve the resilience of our national critical infrastructure. In this light, we strongly urge Congress to pass bipartisan legislation that provides and safeguards much needed, long-term investments in America's competitiveness and technological future.

The Senate's United States Innovation and Competition Act and the House's America COMPETES Act both contain provisions that should be included in any final legislation to counter the Chinese government's ambitions for global technological dominance. We were glad to see both the House and Senate include the full \$52 billion in funding for the CHIPS Act in their respective pieces of legislation to support domestic semiconductor production. Congress passed the CHIPS Act on a bipartisan basis as part of the FY2021 National Defense Authorization Act. Now, the House and Senate stand ready to fund the CHIPS Act's provisions at levels that will solidify American global leadership in semiconductor technology for the coming decades. This vital investment will carry important benefits to America's cybersecurity and critical infrastructure. For these reasons, we strongly urge that the final legislation include full funding for the CHIPS Act, along with guardrails that ensure companies receiving CHIPS funding do not expand their footprint in China.

We also urge the inclusion of several other essential cybersecurity provisions which the House and Senate bills share. Both address shortages in the federal cyber workforce with investments in STEM education, including the Cybersecurity Opportunity Act, and create rotational cybersecurity positions to give federal employees the flexibility to gain experience and skills. Both bills invest in U.S. leadership in international technical standards-setting bodies where the Chinese Communist Party seeks to displace Western-aligned values of a free and open internet

without control and censorship. Both bills also increase funding for the State Department's Global Engagement Center, which is an important program for battling foreign disinformation campaigns.

Each of the two bills also contains unique measures that are essential to strengthening American cybersecurity and resilience for the 21st century. We strongly recommend that the House and Senate work to reach agreement on these measures for inclusion in the final conferenced bill.

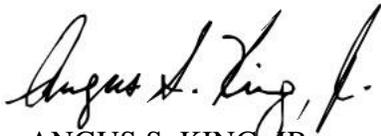
The House bill contains bipartisan language which would reduce American dependency on untrusted vendors beholden to foreign powers by requiring the President to develop a strategy for information and communication technology critical to the economic competitiveness of the United States. It would also strengthen America's local, state, and federal cybersecurity workforce by expanding CyberCorps: Scholarship for Service, a proven ROTC-like program for recruiting and developing cybersecurity talent to work at all levels of government. The House bill would further improve the security of America's software and technology ecosystem by supporting the software security and digital privacy work of the National Institute of Standards and Technology, and designating Critical Technology Security Centers to evaluate and test the security of technologies essential to national critical functions. Finally, the House bill would create international capacity-building programs to improve the cybersecurity of U.S. allies and partners.

For its part, the Senate bill would create a National Risk Management Cycle to identify, assess, and prioritize cyber and physical risks to critical infrastructure – something the United States has long required, but long lacked. In our March 2020 report, the Cyberspace Solarium Commission noted that the U.S. government “lacks a rigorous, codified, and routinely exercised process” for identifying risk. By creating a National Risk Management Cycle, Congress would codify an essential capability for properly resourcing U.S. government efforts to deter threats and mitigate risks to critical infrastructure. The Senate legislation would also invest in America's technological future by creating regional technology hubs, built on partnerships among industry, academia, and workforce groups, to support domestic high-tech job growth in areas of the country that have not been historic innovation centers.

Congress has a critical opportunity to advance and secure U.S. global technological leadership for the 21st century. In doing so, it must also invest in America's cybersecurity and critical infrastructure resilience. The cyber threats facing our country have never been greater, and American technological leadership will depend significantly on our ability to defend against those threats and recover quickly from disruptions to critical infrastructure. As such, we strongly urge that the provisions we have highlighted here be included in the final conferenced legislation that crosses President Biden's desk later this year.

Thank you for your full and fair consideration of this request. We look forward to Congress' passage of this vital piece of legislation.

Sincerely,

Handwritten signature of Angus S. King, Jr. in black ink.

ANGUS S. KING, JR.
United States Senator

Handwritten signature of Mike Gallagher in blue ink.

MIKE GALLAGHER
Member of Congress