ANGUS S. KING, JR.
MAINE

133 HART SENATE OFFICE BUILDING (202)
224-5344
[illegible]

United States Senate

WASHINGTON, DC 20510

ARMED SERVICES
CHAIRMAN, STRATEGIC FORCES SUBCOMMITTEE
ENERGY AND NATURAL RESOURCES
CHAIRMAN, NATIONAL PARKS SUBCOMMITTEE
INTELLIGENCE
VETERANS AFFAIRS

September 27, 2023

The Honorable Jack Reed
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable Mike Rogers
Chairman
Committee on Armed Services
US House of Representatives
Washington, DC 20515

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
US House of Representatives
Washington, DC 20515

Dear Chairman Reed, Chairman Rogers, Ranking Member Wicker, and Ranking Member Rogers:

As the Senate Armed Services Committee (SASC) and House Armed Services Committee (HASC) pursue a final version of the Fiscal Year (FY) 2024 National Defense Authorization Act (NDAA), we who have served on the Cyberspace Solarium Commission respectfully request the conferees give due consideration to several critical provisions, as highlighted in this letter. We also stand ready to provide insights or recommendations to you and your staff on a multitude of additional provisions, if advantageous.

One of our highest priority issues is Senate Section 331, which would establish a pilot program that tests the cyber resiliency and reconstitution of military installations in the event of an attack on their critical infrastructure. This would help prepare installations for a possible cyberattack and map their reliance on critical infrastructure providers. Furthermore, the lessons learned from this program can create a holistic roadmap that addresses any inconsistencies or underperformances across installations.

We support the continued efforts to improve the cybersecurity of the nuclear command, control and communication programs reflected in Senate Section 1717 and House Section 3113. Among other efforts this will develop and direct the implementation of a threat-driven cyber defense construct for systems in this critical mission, as well as a cross-functional team will work to enhance cyber defense. This should also include House Section 1501, which establishes a "Strategic Cybersecurity Program" to ensure the ability of the Department of Defense to conduct its most critical military missions, to include nuclear deterrence, conventional long-range strike, offensive cyber operations, and homeland missile defense.

We also strongly support the many provisions addressing the readiness and personnel shortfalls across all the Services in our cyber forces that impact force generation. We remain anxious that each service has not yet generated the forces needed to support their own manning requirements and CYBERCOM's requirements, including recruiting, retention, and career management of military and civilian personnel in the Cyber Mission Force (CMF). We reaffirm existing statutory reporting requirements including the Section 1502 Report and the Senate Armed Services Committee report accompanying the Senate-

passed bill that requires the Services to report on their progress towards meeting cyber personnel requirements. We support an independent study that examines under Senate Section 1708, leaving all options on the table to improve cyber personnel readiness and force generation model options. There are also several provisions that would enhance the readiness and effectiveness of U.S. Cyber Command and the Services. In addition, we support provisions that enhance the workforce. These provisions include:

- Senate Section 1701 requiring a plan to create common standards for personnel
- House Section 1534, which aims to conduct an internal study on the personnel and resources necessary to improve the occupational resiliency of the Cyber Mission Force.
- House Section 1533, which would authorize the Government Accountability Office to review cyberspace operations management.

To better employ our nation's cybersecurity talent, a civilian cybersecurity reserve should be established under the Department of the Army as outlined in Senate Section 1216. This program would expand the pool of talent the Army could draw on to defend against malicious cyber activity. Similarly, the inclusion of related text in House Section 1122 calling for a National Digital Reserve Corps, further highlights the importance of this issue. As the frequency of cyberattacks increases, a reserve of cybersecurity professionals may be the reinforcements we need in a cyber conflict.

Another vital component to combatting cyber threats is to have rigorous standards for cyber incident reporting. As such, we support Senate Section 1715, which would assign responsibilities to oversee incident reporting, increase incident visibility within the department, and provide new guidance on reporting procedures.

Additionally, we lend our support to the efforts found in Senate Sections 1714 and 1720, which aim to develop much-needed cyber strategies. Section 1714 would establish regional cybersecurity strategies for each of the geographic combatant commands, increasing their readiness for cyber threats in their respective regions. These strategies would streamline cyber capacity building efforts in the geographic commands and identify region-specific cyber threats, among other features. Section 1720 would develop and implement a strategy to bolster the cybersecurity efforts of the Department of Defense's space systems. This would be a department-wide effort that would establish standards for cyber protection and mitigate vulnerabilities of new and legacy space systems, reducing the risk of malicious actors from targeting these necessary systems in a conflict. The establishment of these strategies would provide proactive, rather than reactive, approaches to cybersecurity challenges in their respective sectors.

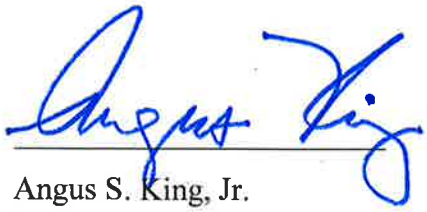
Another key priority of ours is the military cybersecurity cooperation with Taiwan found in Senate Section 1352 and House Section 1505. This provision allows the Secretary of Defense to carry out efforts to protect Taiwan's military networks, infrastructure, and systems from cyber threats, and conduct joint training exercises to educate and strengthen both Taiwanese and U.S. cyber operatives. As Taiwan faces increased attacks from malicious cyber actors, we believe it is imperative that its cyber capacity improves to compete with its cyber adversaries. We appreciate seeing a similar provision provided in House Section 1505, showing greater emphasis on this issue.

Finally, we support the numerous provisions to support the development of ally and partner cybersecurity capacity, beyond that of Taiwan. This includes DoD efforts in Senate Sections 1346 (Southeast Asia), 1399E (Middle East), and 1399DDDDD (Western Hemisphere), and the effort to establish appropriate funding authorities at the State Department in Senate Section 6307.

Thank you for your consideration of these matters. We are grateful for your commitment to U.S.

national security and cybersecurity, and for your diligent work leading these important committees.

Sincerely,



Angus S. King, Jr.
United States Senator

Michael J. Gallagher
United States Representative