

Congress of the United States
Washington, DC 20515

April 04, 2022

The Honorable Joseph R. Biden
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500-0005

Dear President Biden:

One of the most important improvements in our national cyber capability over the past four years has been the development of effective, timely planning processes for the execution of offensive cyber operations. As the Co-Chairmen of the Cyberspace Solarium Commission, we are very concerned by press reporting that your Administration may be considering changes to the governing policy document, National Security Presidential Memorandum – 13, with an intent to limit the Secretary of Defense’s freedom of action to plan and conduct offensive cyber operations.

These improvements in offensive cyber operations were enabled by the passage of the Fiscal Year 2019 National Defense Authorization Act (NDAA) which we both drafted and supported. The law addressed this issue in three areas: it “affirmed the authority of the Secretary of Defense to conduct military activities and operations in cyberspace”, in Section 1632; it established a policy for the use of offensive cyber operations to “deter if possible, and respond to when necessary” adversary cyber operations, in Section 1636; and it provided specific authorities to “conduct active defense” against China, Russia, North Korea and Iran, in Section 1642. Congress’s intent was clear – the United States needed to be more agile and forward in the conduct of offensive cyber operations.

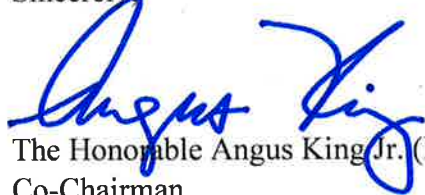
After passage of the NDAA in August 2018, the Trump Administration created NSPM-13, establishing a more agile process for the government to make decisions and gain approvals for offensive and defensive cyber operations. While the process can be utilized by various departments or agencies, it principally allowed for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace.

These new policies were then reportedly used with great effect to limit Russian cyber-enabled information operations against the United States election infrastructure in both 2018 and 2020. They also play an important role in signaling our willingness to use cyber capabilities, a key aspect to an effective national cyber strategy.

The Cyberspace Solarium Commission has worked closely with your Administration, and your predecessors, to ensure that we are ready to respond to significant cyber-attacks against our national critical infrastructure and democratic institutions. We have long argued that this requires three lines of effort: building a more resilient and defended cyber infrastructure, establishing an effective public-private collaboration, and ensuring we have a credible, capable deterrent, including offensive cyber capabilities. Any effort to alter and possibly weaken NSPM-13 signals to our adversaries a lack of credible willingness to use offensive cyber capabilities which undermines the credibility of our deterrent.

It is for these reasons we urge in the strongest possible terms that you to not alter the existing processes and policies that allow for an agile, effective planning process for the conduct of offensive cyber operations – the security of our national critical infrastructure may very well depend upon it.

Sincerely



The Honorable Angus King Jr. (I-ME)
Co-Chairman
Cyberspace Solarium Commission



The Honorable Mike Gallagher (WI-08)
Co-Chairman
Cyberspace Solarium Commission

Cc:

The Honorable Lloyd Austin, Secretary of Defense
Mr. Jake Sullivan, Assistant to the President for National Security Affairs
Mr. Chris Inglis, National Cyber Director