Cyberspace Solarium Commission: “The Covid-19 pandemic illustrates parallels to a significant cyber attack and urges swift implementation of key recommendations.”

Posted on Wednesday, Jun 3, 2020

Washington, D.C (June 2, 2020) – U.S. Senator Angus King (I-Maine) and Congressman Mike Gallagher (R-Wis.), co-chairs of the Cyberspace Solarium Commission (CSC), today announced the release of a new Cyberspace Solarium Commission white paper, “Cybersecurity Lessons Learned from the Pandemic.” While many of the challenges identified in this white paper and the Commission’s final report have existed for the better part of four presidential administrations, the pandemic highlights the relevance of many of the Commissioners’ earlier recommendations in its Final Report that was published in March 2020 detailing a strategy of “layered cyber deterrence.” This new document provides fresh observations from the pandemic as they related to the security of cyberspace, both in terms of the unique cybersecurity challenges it creates, but also what it can teach the United States about how to better prepare for a major cyber disruption.

In examining the impact of the Pandemic, the Commission identified three unique challenges to cybersecurity: the cybersecurity challenges in the new work from home economy,

the risk in increased digitization of critical services, and the impact of opportunistic cybercrime. As the need for social distancing causes small to medium-sized businesses to move their operations online, the increase in reliance on cloud-services underscores the need for those services to be secure. With America working from home more than ever before, the importance of secure in-home and consumer information technology devices has also increased. The rise in opportunistic cybercrime that spawned from the pandemic illustrates the need for robust law enforcement capabilities and authorities.

The pandemic response is also instructive in demonstrating how the United States can best prepare for a major cyber disruption that could occur in the near future. First, it highlights the importance of national leadership and planning to coordinate domestically and engage internationally in the event of a cyber event. Second, preparedness efforts led by the government are of utmost importance to ensure the availability of critical resources and a workforce ready to aid in response and recovery efforts. Third, data-driven prevention and mitigation approaches are extremely helpful in mitigating national risk. Fourth, the U.S. government must have response and recovery capability and capacity to coordinate, respond to, and recover from crises. Finally, viral disinformation represents a harsh challenge that can be countered by building societal resilience and empowering organizations that identify, expose, and explain those operations.

“The coronavirus pandemic has hammered home just how important it is to prepare for a crisis before it occurs rather than once it strikes,” **said Senator King.** “Additionally, the ongoing social distancing requirements have increased America’s already-high reliance on our digital infrastructure, which is central in everything from working to paying bills to grocery shopping. I’ve long said that structure is policy, and by making investments in digital security, pursuing organizational reform, getting the right personnel into place, and creating a clear gameplan to deter bad actors, we can improve our readiness to

protect our nation from those who would wish to transform cyberspace into a battlefield. The need for action is clear – so let's act."

"The Coronavirus has magnified the important role that cyber infrastructure plays in our economy, and how incredibly disruptive a catastrophic cyber attack would be to our every day life " **said Rep. Gallagher.** "Amidst these parallels, the Commission's report is more important than ever. We are woefully unprepared for a cyber calamity, and absent decisive investment in prevention and risk mitigation, our nation could be crippled by a major attack. Thankfully, we still have time to heed the Commission's recommendations and strengthen our cyber resiliency. If we do, we will be in a much better position to not only coordinate a whole-of-nation response to a significant cyberattack, but to prevent them in the first place. As the Coronavirus has shown, an ounce of prevention is worth a pound of cure."

The full white paper can be read HERE.

The white paper highlights 32 of the Commission's original recommendations. These recommendations include:

- Establishing a **National Cyber Director** to coordinate the federal government's incident response activities and serve as the focal point for private sector leaders to engage the executive branch on cybersecurity issues,
- Substantially modifying the Commission's original recommendation to **expand the update of secure cloud services** to now call on Congress to **include digitization grants to state, local, territorial, and tribal governments as part of COVID-19 stimulus**,
- Developing and maintaining **continuity of the economy planning** to ensure continuous flow of goods and services regardless of a disruption's cause, and
- Building **societal resilience to disinformation.**

The white paper also notably adds four new recommendations. These include:

- Urging Congress to **pass an Internet of Things Security Law**
- Increasing support to nonprofits that **assist Law Enforcement efforts to combat cybercrime and support victims**
- Support for establishing a **Social Media Data and Threat Analysis Center**
- Increasing **nongovernmental capacity to identify and counter foreign disinformation and influence campaigns.**

The current pandemic is a wake-up call about the challenge of non-traditional national security emergencies. For four presidential administrations, the United States has watched as adversaries attempt to hack into its critical infrastructure, steal its intellectual property, influence democratic institutions, and interfere in its economy. Yet again, this crisis is being exploited by threat actors to disrupt critical systems, spread disinformation, and more. This pandemic is causing the United States to experience firsthand what could happen in the event of a major cyber event. Now is the time to heed these lessons, and strengthen America's cyber resilience.

A CSC staff-led discussion of this event will happen on Wednesday, June 3, at 12 PM EDT. To RSVP, please register here.

###