COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Opening Statement of Rep. James R. Langevin (D-RI)

Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Hearing

Defending Against Future Cyberattacks: Evaluating the Cyberspace Solarium Commission Recommendations

July 17, 2020

I had the privilege of serving on the Solarium Commission with the witnesses testifying here today, and I can honestly say that working on our report was one of the highlights of my Congressional career. Our thoughtful research, outreach, and deliberation was a testament to our two co-chairs, Senator King and Congressman Gallagher, and I hope our subcommittee takes full advantage of the wealth of knowledge at the virtual witness table.

The Commission's report outlines a strategy of layered cyber deterrence and includes 82 recommendations on how the government can implement that strategy. I am looking forward to discussing those recommendations with my colleagues today – particularly those that would strengthen the Cybersecurity and Infrastructure Security Agency by increasing its capabilities and clarifying its relationship with the intelligence community and sector specific agencies.

I am also looking forward to covering the essential role of Congress in improving our nation's cybersecurity posture. From the outset of the Commission – and thanks to the work of our dedicated Executive Director, Mark Montgomery – we deliberated with a bias toward action. After all, as the members of this subcommittee know full well, the status quo in cyberspace sees us making steady progress while the threat increases exponentially.

We need to act, and act now, to change that dynamic and get ahead of the curve. I am proud to report that leaders on this subcommittee, including Chairman Richmond, Ranking Member Katko, and Representatives Jackson Lee, Rice, Slotkin, Green and Joyce all have amendments to the forthcoming National Defense Authorization Act to implement aspects of the Solarium report. It is an honor to share the (virtual) dais with members committed to addressing this quintessential Information Age challenge, and I am sure the Committee – and this subcommittee – will continue to play a vital role in implementing the report.

I encourage our witnesses to discuss why Congress is so important to moving the conversation forward on cybersecurity. And I encourage my colleagues to probe the decision-making behind the strategy and the recommendations.

The events of this year provide an interesting context in which to review the Solarium Commission's recommendations. The COVID-19 pandemic has upended and altered the way we live, the way we work, and the way we govern. Almost overnight, nearly half of employed adults became teleworkers, putting added stress on our infrastructure and creating new opportunities for hackers to wreak havoc.

Now Congress is holding remote hearings, and State and local governments have become e-governments with little time to transition. Many state and local governments are also finding, that due to antiquated IT systems and the fact that their data aren't in the cloud, they are unable to scale and secure vital programs like unemployment insurance, highlighting the need for modernization as part of the security push.

Our adversaries have noticed the broader attack surface. Just yesterday, CISA – in conjunction with allies in the UK and Canada – announced that Russian operatives are targeting health care organizations doing research on the virus. And two days ago, we saw a major breach of Twitter that saw many prominent accounts linking to a Bitcoin scam. It doesn't

take much imagination to see what chaos one could sow with such access on Election Day if a bad actor was pushing out disinformation.

The realities of 2020 make clear that a comprehensive, whole-of-nation approach to cybersecurity is a necessity, but we do not yet have one. We lack a clear leader in the White House whose mission it is to focus on cybersecurity. We lack clear understanding of roles and responsibilities, both within government and between government and the private sector. We lack clear metrics to measure our progress.

The Cyberspace Solarium Commission report cannot fix all the challenges we have in cyberspace. But it does chart a bold course, and it does not shy away from the tradeoffs we will need to make to decisively improve our cybersecurity posture. The report makes clear that everyone – from government to private sector companies to Congress itself – needs to make meaningful changes.

We need to expect more from government: closer coordination across agencies, stronger collaboration with critical infrastructure, and, critically, a greater emphasis on planning. And we need to strengthen government agencies – in particular CISA – to do so.

We also need to expect more from the private sector. We need companies to truly accept the risks they take in cyberspace by accepting the consequences of failing to protect their data and networks. We also need technology companies – what the report calls "cybersecurity enablers" – to do more to make the secure choice the default choice. Too often, we see a rush to be first to market, not secure to market. Too often, we see entities like ISPs not protecting their small and medium sized customers because they don't believe it's their job.

Most importantly, where the public and private intersect, at the nexus of critical infrastructure that this committee is charged with protecting, we need to ensure the private sector is doing its part to protect itself while acknowledging that they can't go it alone.

This is part of the end state we desire in the Solarium report, a state where we are resilient enough to deter our adversaries and agile enough to push back when they insist on testing our defenses. That end state is in reach, but it will require the work of this subcommittee – and of the experts we have invited before us – if we are to achieve that goal.

# # #

Media contact: Adam Comis at (202) 225-9978