COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Chairwoman Yvette Clarke (D-NY)

Mobilizing Our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure

April 6, 2022

I would like to thank the witnesses for participating in today's hearing on how we can build a better, more robust framework for protecting our nation's most critical infrastructure. As some of you may know, this is not my first time serving as Chair of this Subcommittee. The last time I presided over this panel was in 2011, during the 111th Congress.

At the time, the Obama Administration was working to develop, and strengthen, many of the policy frameworks we know today – which place DHS at the center of a voluntary, public-private partnership to promote strong cybersecurity across sectors. I've also served as Ranking Member of this Subcommittee, working across the aisle to codify many of those voluntary frameworks and information sharing regimes. With that backdrop in mind – and with all due respect to the hard work that's been done – I think it's time to be candid about the limits of these voluntary partnerships and authorities.

When I rejoined the Subcommittee last year, we were reeling from a massive supply chain attack that gave Russia months of access to some of our most critical networks. We've had to watch from the sidelines as our critical infrastructure – from hospitals and meatpackers to manufacturers and pipelines – have been crippled by ransomware attacks.

For the past few months, Federal officials – like the ones on our panel today – have been working around the clock to help private sector owners and operators understand that they may soon be the target of retaliatory Russian cyberattacks. But we have no way of knowing if these operators are hearing those warnings and taking action to shore up their defenses. From where I'm sitting, one thing is clear, the U.S. desperately needs to revamp the playbook it uses for critical infrastructure cybersecurity.

We know that our nation's critical infrastructure is vulnerable to cyberattacks – and the Federal government has resources it can bring to bear in closing security gaps. But we've been reluctant to make the private sector to come to the table. The Federal government also has the bird's eye view vantage point to track cyber threats in one sector, then use that information to connect the dots on other malicious activity across sectors. But until recently, we haven't been willing to require critical infrastructure operators to provide that information to CISA.

While the Biden Administration has taken some aggressive steps to partner with the private sector in new, innovative ways – we have a long way to go, and some big challenges ahead. Fortunately, we know that Congress can still come together to tackle big challenges. My recently enacted cyber incident reporting legislation is proof of that.

To get this legislation across the finish line, we had to work across the aisle, and with our partners in industry, to find a solution that would give CISA the visibility it needs without needlessly burdening

victims of a cyberattack. We found a smart, compromise solution there – and I have faith we can do it again here. My goal today is to get testimony that will help us answer the question – what's next?

How do we continue to mature the way the government engages with critical infrastructure – particularly those entities that are the "most critical of the critical"? Or, as the Cyber Solarium Commission put it, our "Systemically Important Critical Infrastructure," or SICI? Do we have a good sense of where these SICI assets are, who's operating them, and how they're being secured?

And, once we know who and what they are – what benefits should the Federal government provide for these entities to help them protect themselves? And, importantly, what burdens should they be asked to shoulder, in light of their importance to our national security?

This latter part is key. It is not enough to simply identify these "most critical" entities – nor is it consistent with what the Solarium Commission proposed. We need to be able to answer the question: what do these companies need to do as a result of their designation? And what does the Federal government need to do for them – whether that's better access to threat intelligence, enhanced operational collaboration, or other priority access to resources and support?

It's not enough to simply make a list of our most vital assets – we need to know how we're going to operationalize it. We've tried this exercise in 'list-making' before – from the National Asset Database, to the designation of "Section 9" companies. Some of these efforts were costly and labor-intensive, and none of them ever really lived up to the security gains originally envisioned. The through line for all these efforts is that at some point, Congress, or the Administration, or both, decided to punt on the question of benefits and burdens. That will not happen on my watch.

I would like to recognize Representative Langevin and Ranking Member Katko for championing this issue, and I look forward to continuing to work with them to craft this legislation in a way that avoids the pitfalls of the past. This hearing is an opportunity to help move the ball forward and hear how the Administration is thinking about these challenges and working to upgrade its cybersecurity playbook.

# # #

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