Opening Statement as Prepared for Delivery
By The Honorable Susan M. Gordon
Former Principal Deputy Director of National Security

10 February 2021

Good afternoon, Chairman Thompson, Ranking Member Katko, and distinguished members of the committee. Thank you for the opportunity to testify on this issue of national security interest—cybersecurity and resilience. It's great to see you again, even as a private citizen not your Principal Deputy Director of National Intelligence.

Though my colleagues and I sitting before you all come from different backgrounds and have different perspectives on the issue, I think we all believe there is little more important work we can do as a Nation and as a free and open society than that which you are tackling here today and in the coming days.

I am here to discuss three aspects of the issue: the **nature of the cyber threats** we face and that are emerging, the **domains in which those threat manifest**, and **the imperatives that must drive solution**. My colleagues will discuss the specifics of recent attacks and proffer specific next steps, I hope to put those in context.

First, in terms of threat, offensive cyber capability is a global commodity—the means by which every interest of our adversaries and competitors is increasingly achieved. In a digitally connected world, one need not travel great physical distance or expend great resource to achieve malign outcome.

15 years ago, offensive cyber was the tool of the great powers, wielded in a largely unconstrained environment, with very specific, narrow intention against governmental interests. Today, it is the tool of criminals, nation states, and non-nation state actors, and while some are more capable than others in achieving strategic impact, all are capable. In the hands of malign actors, it can have physical, political, military, economic, and societal impact, as we have witnessed just this past year with ransomware attacks intellectual property theft, and theft of PII, disinformation campaigns, intelligence collection activity, and disruption of service.

We need to stop acting like it's special, or rare, or somehow beyond our ken or ability to respond because it's happening digitally. This digital activity has physical consequence. The outcomes that cyber actors are producing threaten our national security.

Second, in terms of domain, it used to be that governments held all the vital information (kept the secrets worth stealing) and wielded all the power (made all the decisions worth influencing.) No longer. The engine of our great society lies in our companies and our communities, and the decisions made in board rooms and voting booths can have global impact, so the threat surface includes private companies and private citizens, and their

decisions can have direct effect on National security as surely as it would if they held government position.

Threat actors today target government and non-government, critical infrastructure and private citizens, academic institutions and research centers, huge multi-national corporations and small businesses. While in some cases the victim is the target, sometimes they are just the transportation and access to the intended quarry. Said differently, if you aren't the target, you might be targeted—no one gets off free. But most of all, what we're seeing today are attacks on the most important aspect of free and open societies—trust—and we cannot allow that to continue.

Success of the opportunistic predator often can be thwarted by the cyber equivalent of locking the front door and putting your valuables in a safe. But in the case of relentless pursuers—most likely nation-states with massive resources and strategic patience—success can only be thwarted by understanding the intention of the actor and committing to whole of organization, whole of nation, whole of society persistent attention to risk management.

Third, enough problem identifying. Your purpose—our collective purpose—is to find solution.

Let me offer some imperatives or "first principles" to guide next steps.

- Solutions cannot be exclusively federal, or exclusively governmental, or exclusively US
- Solutions cannot be exclusively technical
- Solutions cannot be only for the resource rich
- Solutions cannot focus solely on single entities
- Intelligence must be more widely, more openly shared, especially about intent
- Bring the problem into the light, ruthlessly, because evil can't survive there

To close out with these principles in mind, and in the pursuit of solutions, I offer that we must approach today's rapidly changing threat posture with continually evolving defense practices. Where we previously focused on tangible threats, we must now constantly be adapting to the challenges presented by the digital world. To achieve this defensive agility, the intelligence community, government, industry, and must work closer together.

I look forward to your questions.

Thank you.