OPENING STATEMENT

Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"*Strengthening U.S. Cybersecurity Capabilities*"
February 14, 2017

Thank you Chairwoman Comstock. I look forward to working with you and all of the returning and new Members of the Research & Technology Subcommittee in this new Congress. Thank you also to the distinguished panel for being here this morning to share your expertise on this important topic.

Cybersecurity has long been a priority of mine in Congress. The *Cybersecurity Enhancement Act of 2014*, which was signed into law, began as a bill that Rep. McCaul and I introduced in 2009. As pointed out in the CSIS report, cybersecurity is a topic on which nearly every Committee in Congress has something to contribute. [On one hand, this presents a challenge to developing and enacting comprehensive and coherent policies. On the other hand, it presents an opportunity for coordinated policy making across the government to address this complex and pressing issue.]

Our committee is uniquely positioned to contribute meaningfully to oversight and policy development for cybersecurity because of our jurisdiction over NIST, and our oversight responsibility for STEM education and workforce training activities across the Federal government. I understand that today's hearing is likely just the first of several hearings on cybersecurity we will hold this Congress, and as such it is intentionally broad in scope. However, sitting before us are a few of our nation's top experts on NIST's role in cybersecurity and on cybersecurity education and workforce issues, so I look forward to hearing those specific areas from our witnesses.

NIST plays a central role in the security of federal information systems. The experts at NIST develop the security standards and guidelines that all other civilian federal agencies are required to implement through the Federal Information Security Modernization Act, or FISMA. Those experts also provide technical assistance to other agencies. Furthermore, NIST led the development of the Cybersecurity Framework for Critical Infrastructure, a widely adopted set of

voluntary guidelines and standards for industry, and works closely with industry to help develop tools for businesses of all sizes and from all sectors to effectively implement the Framework.

There have been some calls for an expanded role for NIST, including an expanded oversight role under FISMA. These suggestions warrant careful examination. NIST is successful in its current role in large part because of its independence as a standards and technology agency, and not a regulatory or enforcement agency. Any discussion about an expanded role must be accompanied by a discussion about increasing resources.

On the topic of education and workforce, NIST leads Federal efforts through coordination of the National Initiative for Cybersecurity Education, or NICE. Another agency in our jurisdiction, the National Science Foundation, supports important programs such as the CyberCorps Scholarship for Service. However, the gap between supply and demand for cybersecurity training in both the government and the private sector remains an urgent challenge. All of the best policies are meaningless without the skilled workforce to implement those policies. Increasing the recruitment and retention of cybersecurity talent in our Federal agencies is going to require new and creative thinking, as well as increased resources. It is also going to require stepping back from the disparaging rhetoric aimed lately at the civil service. Federal agencies already struggle to recruit and retain top talent from the limited pool of qualified cybersecurity professionals, especially when private sector salaries are much higher. Negative remarks, combined with a federal hiring freeze, do real damage to agencies' recruitment and retention efforts.

Once again, I want to thank the Chairwoman for holding this hearing, and the witnesses for sharing your time and expertise with us this morning. I look forward to your testimony.

I yield back.