OPENING STATEMENT

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

Committee on Science, Space & Technology
Subcommittee on Oversight
Subcommittee on Research & Technology
"Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry"
June 15, 2017

Thank you Chairman LaHood and Chairwoman Comstock for holding this hearing on cybersecurity and lessons learned from the WannaCry ransomware attack last month.

The good news is that U.S. government information systems were not harmed by the WannaCry attack. This was a clear victory for our cyberdefenses. However, I believe there are lessons to be learned from successes as well as failures. A combination of factors likely contributed to this success, including getting rid of most of our outdated Windows operating systems, diligently installing security patches, securing critical IT assets, and maintaining robust network perimeter defenses. As we know, Microsoft sent out a security patch for this vulnerability in March, two months before the WannaCry attack. These and other factors played a role in minimizing damage to U.S. businesses as well.

However, WannaCry and its impact on other countries serves as yet another reminder that we must never be complacent in our cybersecurity defenses. The threats are ever evolving, and our policies must be robust yet flexible enough to allow our defenses to evolve accordingly.

The Federal Information Security Modernization Act, or FISMA, laid out key responsibilities for the security of civilian information systems. Under FISMA, DHS and OMB have central roles in development and implementation of policies as well as in incident tracking and response. NIST develops and updates security standards and guidelines both informing and responsive to the policies established by OMB. Each agency is responsible for its own FISMA compliance, and each Office of Inspector General is required to audit its own agency's compliance with FISMA on an annual basis. We must continue to support agencies in their efforts to be compliant with FISMA while conducting careful oversight.

In 2014, NIST released the Cybersecurity Framework for Critical Infrastructure, which is currently being updated to Framework Version 1.1. While it is still too early to evaluate its full impact, it appears the Framework is being widely used across industry sectors. Our Committee recently reported out a bipartisan bill, H.R. 2105, that I was pleased to cosponsor, that would ensure that the Cybersecurity Framework is easily usable by our nation's small businesses. I hope we can get it to the President's desk quickly. In the meantime, the President's recent cybersecurity Executive Order directs Federal agencies to use the Framework to manage their own cybersecurity risk. As we have heard in prior hearings, many experts have called for this step, and I applaud the Administration for moving ahead. I join Mr. Beyer in urging the

Administration to fill the many vacant positions across our agencies that would be responsible for implementing the Framework as well as shepherding the myriad reports required by the Executive Order.

Finally, I will take this opportunity to express my disappointment in the Administration's budget proposal for NIST. The top-line budget cut of 25 percent was so severe that if it were implemented, NIST would have no choice but to reduce its cybersecurity efforts. This represents the epitome of penny-wise, pound-foolish decision making. NIST is among the best of the best when it comes to cybersecurity research and standards, and our modest taxpayer investment in their efforts helps secure the information systems not just of our federal government, but our entire economy. I trust that my colleagues will join me in ensuring that NIST receives robust funding in the FY18 budget and doesn't suffer the drastic cut requested by the President.

Thank you to the expert witnesses for being here this morning. I look forward to your testimony. I yield back.