COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
June 15, 2017

Media Contact: Kristina Baum
(202) 225-6371

Statement of Chairman Darin LaHood (R-Ill.)
Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry

Chairman LaHood: Good morning and welcome to today's joint subcommittee hearing: "Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry."

I would like to welcome Chairman Smith, Oversight Subcommittee Ranking Member Beyer, Research and Technology Subcommittee Chairman Abraham, Research and Technology Ranking Member Lipinski, Members of the Subcommittees, our expert witnesses, and members of the audience.

Cybersecurity—a concept we hear mentioned frequently, especially in this period of rapidly emerging threats—is an ever-evolving concept. Maintaining an effective cybersecurity posture requires constant vigilance as new threats emerge and old ones return. Too often, however, when we hear about the importance of cybersecurity we are left without concrete steps to take to ensure our systems are best positioned to defend against emerging threats. One of the goals of today's hearing is to learn about real, tangible measures the government can take to ensure its IT security systems are appropriately reinforced to defend against new and emerging threats, including novel and sophisticated ransomware threats.

The specific focus of today's hearing will be the recent WannaCry ransomware attack, a new type of ransomware infection, which affected over one million unique systems last month in a worldwide attack that impacted nearly every country in the world.

Although the concept of ransomware is not new, the type of ransomware employed by WannaCry was novel. WannaCry worked by encrypting documents on a computer, instructing victims to pay $300 in bitcoin in order to regain access to the user's documents. Unlike typical forms of ransomware, however, WannaCry signaled the ushering in of a new type of "worming" ransomware, which caused the attack to spread faster and more rapidly with each new infection. In light of the novelty built into WannaCry's method of attack, cybersecurity experts, including those we will hear from today, have expressed significant concerns that WannaCry is only a preview of a more sophisticated ransomware infection that many believe will inevitably be launched by hackers in the near future.

Beginning May 12, 2017, the WannaCry ransomware infection moved rapidly across Asia and Europe, eventually hitting the United States. The attack infected 7,000

computers in the first hour and 110,000 distinct IP addresses in two days and in almost 100 countries, including the U.K., Russia, China, Ukraine, and India. Experts now believe WannaCry affected approximately 1 to 2 million unique systems worldwide prior to activating the kill switch.

Close to my district, Cook County's IT systems were compromised by WannaCry—reportedly one of a few local governments subject to the attack. Although Cook County has worked to appropriately patch their systems, it is important that we ensure that all vulnerabilities are appropriately remedied in the event of a more sophisticated attack.

Fortunately, the hackers responsible for WannaCry mistakenly included a kill switch, which was uncovered by an employee of Kryptos Logic and used to terminate the attack. The Kryptos Logic employee exploited a key mistake made by the hackers when he registered the domain connected to the ransomware attack. Experts estimate that the kill switch prevented 10 to 15 million unique worldwide systems infections and reinfections.

Although based on information available thus far the federal government's systems were fortunately spared from WannaCry, we want to ensure that the government is sufficiently prepared in the likely event of a more sophisticated attack. Additionally, the Committee wants to hear what Congress can do to appropriately address this climate of new and emerging cybersecurity threats.

Through the lens of the aftermath of WannaCry, today's witnesses will help shed light on key steps the government should take to ensure its systems are protected. We will also hear today about how public-private partnerships are an instrumental tool to help bolster the government's cybersecurity posture. Finally, we will learn about how the President's recent cybersecurity order, which makes NIST's cybersecurity framework mandatory on the Executive Branch, is a significant step toward ensuring the federal government's cybersecurity posture incorporates the most innovative security measures to defend against evolving threats.

It is my hope that our discussions here today will highlight areas where improvement is necessary, while offering recommendations as we move forward to ensure the federal government is prepared to respond to emerging cybersecurity threats. I look forward to hearing from our distinguished witnesses.

###