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

For Immediate Release
June 15, 2017

Media Contact: Kristina Baum
(202) 225-6371

**Statement of Chairman Lamar Smith (R-Texas)**
*Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry*

**Chairman Smith**: I would like to thank Oversight Subcommittee Chairman LaHood and Research and Technology Subcommittee Vice Chairman Abraham for holding today's hearing.

In the wake of last month's WannaCry ransomware attack, today's hearing is a necessary part of an important conversation the federal government must have as we look for ways to improve our federal cybersecurity posture. While WannaCry failed to compromise federal government systems, it is almost certain that outcome was due in part to a measure of chance.

Rather than seeing this outcome as a sign of bulletproof cybersecurity defenses, we must instead increase our vigilance to better identify constantly evolving cybersecurity threats. This is particularly true since many cyber experts predict that we will experience an attack similar to WannaCry that is more sophisticated in nature, carrying with it an even greater possibility of widespread disruption and destruction. Congress should not allow cybersecurity to be ignored across government agencies.

I am proud of the work the Committee has accomplished to improve the federal government's cybersecurity posture.

During the last congress, the Committee conducted investigations into the Federal Deposit Insurance Corporation, the Internal Revenue Service, and the Office of Personnel Management, as well as passed key legislation aimed at providing the government with the tools it needs to strengthen its cybersecurity posture.

President Trump understands the importance of bolstering our cybersecurity. He signed a recent Executive Order on cybersecurity, which is a vital step toward ensuring the federal government is positioned to detect, deter, and defend against emerging threats. Included in the President's Executive Order is a provision mandating that Executive Branch departments and agencies implement NIST's Cybersecurity Framework.

While continuously updating its Cybersecurity Framework, NIST takes into account innovative cybersecurity measures from its private sector partners.

NIST's collaborative efforts help to ensure that those entities that follow the Framework are aware of the most pertinent, effective, and cutting edge cybersecurity measures.

I strongly believe the President's decision to make NIST's Framework mandatory for the federal government will serve to strengthen the government's ability to defend its systems against advanced cyber threats like the recent WannaCry ransomware attack.

Similarly, the Committee's NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, sponsored by Representative Abraham, draws on findings from the Committee's numerous hearings and investigations related to cybersecurity. It underscores the immediate need for a rigorous approach to protecting U.S. cybersecurity infrastructure and capabilities.

Like the President's recent Executive Order, this legislation promotes federal use of the NIST Cybersecurity Framework by providing guidance that agencies may use to incorporate the Framework into risk mitigation efforts. Additionally, the bill directs NIST to establish a working group with the responsibility of developing key metrics for federal agencies to use.

I hope that our discussions here today will highlight distinct areas where cybersecurity improvement is necessary, while offering recommendations to ensure cybersecurity objectives stay at the forefront of our national security policy discussions.

###