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

For Immediate Release
March 1, 2017

Media Contact: Kristina Baum
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)
H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017

Chairman Smith: Good morning and welcome to today's Full Committee mark up of an important and timely bill.

In the last Congress, the Science Committee held a dozen hearings related to oversight and policy aspects of federal cybersecurity issues.

The hearings included the examination of data breaches at the Office of Personnel Management (OPM), the Internal Revenue Service (IRS) and the Federal Deposit Insurance Corporation (FDIC).

These hearings underscored the need for a robust approach to protect U.S. cybersecurity capabilities.

Two weeks ago, the Research and Technology Subcommittee held a hearing on this issue where experts testified on recommendations in two recent reports that involve the National Institute of Standards and Technology (NIST).

The bill we consider today, H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, implements key ideas and strengthens federal government cybersecurity. I thank Representative Abraham for his initiative on this legislation.

H.R. 1224 ensures that NIST remains a global leader in cybersecurity knowledge, scientific standards-setting, and research and analysis of federal agencies' cyber security readiness.

This common sense legislation takes advantage of NIST's unique capabilities to both develop cybersecurity standards and guidelines, which NIST does now, and go further and evaluate and assess the extent of federal agencies' compliance with them.

Creating more working groups and guidelines without a determination of whether anyone is using them or using them correctly does not protect our cyber infrastructure.

NIST has the experts who develop the standards and guidelines under the Federal Information Security Modernization Act, which apply to the federal government.

NIST experts also developed a Cybersecurity Framework, through collaborations between government and private sector, that are accepted and used by many

private organizations to address and manage their cybersecurity risks in a cost-effective way.

H.R. 1224 directs NIST to promote the Cybersecurity Framework by providing federal agencies with guidance on how to implement it. Who better to determine if an agency is following these recognized standards than NIST?

We do not make NIST an enforcement agency. The bill does not give the agency authority to exact fines, issue injunctions, or pursue further proceedings beyond assessing, auditing, and reporting.

NIST's assessment, audits, and the resulting reports are for federal agencies only and will not affect the private sector.

We recognize NIST will need resources to accomplish this work. We will address that in a NIST authorization bill this year.

The federal government collects personally identifiable information about every person in our country. Unfortunately, the federal government is the world capital of cyber insecurity.

Two years ago, Chinese hackers broke into OPM's computer systems and stole the personally identifiable information and sensitive background check information of approximately 26 million people, including fingerprint records of 5.6 million individuals.

Chinese cyber-criminals also repeatedly hacked – and may still be hacking – the FDIC computer network. The FDIC hacks threaten everything from large-scale manipulation of our entire financial system to looting individuals' checking, savings, and retirement accounts.

At the IRS, 2016 tax-refund fraud is projected to set a new record at $21 billion. An enterprising crook needs only a name, date of birth and a Social Security number to enter made-up W-2 information, submit a fraudulent return, and receive a refund from the IRS within 30 days.

Unless we take new and aggressive steps to prevent rapidly increasing cyber-attacks by foreign criminals and unfriendly governments, our economy and national security are at risk.

Not doing this is a vote for the status quo, which will allow continued security breaches to occur.

Representative Abraham's bill serves an important purpose and expands our ability to protect Americans from cybersecurity attacks. I again thank him for his work and I urge my colleagues to support H.R. 1224.

###