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

For Immediate Release
April 14, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)

Can the IRS Protect Taxpayers' Personal Information?

Chairman Smith: Thank you Madam Chair, and thanks to our witnesses for being here today.

In this Congress, the Science Committee has held half a dozen hearings on cybersecurity issues and vulnerabilities at federal agencies. And we continue to hear the concerns of millions of Americans who quite frankly don't trust the federal government to protect their personal information from cyber criminals.

Too many federal agencies fail to meet the basic standards of information security. We've seen this with HealthCare.Gov and the cyber breach at the Office of Personnel Management (OPM).

The same is true for the IRS. According to a report published last November by the Treasury Inspector General for Tax Administration (TIGTA), the IRS' identity authentication methods for online services do not comply with Government Information Security Standards.

In other words, the IRS has not taken the necessary steps to ensure that individuals are who they claim to be before handing over Americans' confidential tax information. As a result of these vulnerabilities, the TIGTA report found that, "unscrupulous individuals have gained unauthorized access to tax account information."

The U.S. Government Accountability Office (GAO) has identified a number of ongoing cybersecurity system gaps and IRS failures to fully implement certain security controls. The report found that of 28 prior GAO cybersecurity recommendations to the IRS, nine have not been effectively implemented.

These gaps could open the door for cyber criminals to steal confidential taxpayer data.

The past year's IRS breaches are especially troubling. Taxpayer data was fraudulently accessed, not through a forcible compromise of the computer systems, but by hackers who correctly answered security questions that should have only been answerable by the actual individual.

The hackers likely accessed the requisite data from prior high profile hacks. Last year's OPM and Anthem Health Insurance breaches compromised the information of over 100 million people. This included the names, addresses, dates of birth, and Social Security numbers of the victims.

For cyber criminals, this information is similar to making duplicate keys to your house. It's a license to steal whenever and wherever the criminals find an opportunity. The IRS security breach demonstrates once again that rigorous adherence to all cybersecurity protections must be the top priority for every federal agency.

Slow responses and partial measures at the IRS do not protect innocent Americans from these cyber-attacks. The government should be accountable to the people and keep Americans' sensitive information secure.

Thank you and I yield back.

###