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

For Immediate Release
April 14, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Research & Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)

Can the IRS Protect Taxpayers' Personal Information?

Chairwoman Comstock: As the deadline to file taxes winds down, the only question on taxpayers' minds should be when they will receive their tax refund, and not whether someone else has already beaten them to it. I should know – I received a letter from the IRS earlier this year informing me that my account was compromised. But recent news reports and audits of the Internal Revenue Service by the Treasury Inspector General for Tax Administration, or TIGTA, and the U.S. Government Accountability Office (GAO) would suggest otherwise.

On May 26, 2015, the IRS announced that criminals had gained unauthorized access to taxpayer information through its online "Get Transcript" application by accurately answering taxpayers' security questions. At first, as it shut down the application, the IRS claimed that around 100,000 taxpayers' accounts had been accessed out of about 200,000 total attempts. Since then, those numbers have been revised to approximately 340,000 in August 2015, and as of this February, to over 700,000 taxpayers who have had their personal and tax data stolen.

The theft of this data enabled hackers to access information from prior tax returns which resulted in fraudulent tax claims. Approximately 15,000 of the fraudulent tax claims were successfully filed with the IRS leading to an estimated $50 million in illicit refunds.

Then on March 7, 2016, the IRS suspended the Identity Protection Personal Identification Number – or IP PIN – application due to security concerns.
The IRS began issuing IP PINS five years ago to victims of identity theft as an additional layer of security when they filed their taxes. But the system to protect the IP PIN application was the same as the "Get Transcript" application that was hacked last year.

While the IRS suspended the "Get Transcript" application in May, it did not suspend the IP PIN application until last month, during which time at least one individual had her taxpayer information stolen and used to file a fraudulent tax return.

I understand and sympathize with the frustrations of the American public over these incidents. And what makes matters worse is that no one had to break into the IRS system to access information. Instead, the criminals used information from other

cyber-attacks to accurately answer questions on the IRS website to access information they should not have been able to access, and may not have been able to access had the agency followed security guidelines provided by the National Institute of Standards and Technology (NIST).

This ostensible lack of compliance with NIST guidelines is disconcerting. While I appreciate the IRS' efforts to accommodate most people's desire to access their tax information electronically, it cannot do so at the expense of their security. As someone whose information was compromised in last year's OPM hack, I assure you, more security is better than less. This would also help many of my federal employee constituents who were impacted by the OPM breach, as well as by last year's Anthem cyber-attack. As one of the largest health insurance providers in the Commonwealth, the Anthem hack hit particularly close to home for us too.

I look forward to hearing from our witnesses and I thank you all again for being here today.

###