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

For Immediate Release
September 13, 2016

Media Contacts: Kristina Baum
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)

Protecting the 2016 Elections from Cyber and Voting Machine Attacks

Chairman Smith: We are here today to discuss the subject of election security. It's hard to imagine a more bipartisan issue. Election security is fundamental to the fairness of elections and democracy in the United States.

Elections are a key component of democracy, and voting is the very essence of what President Abraham Lincoln meant when he said a government "*by the people*."

Voting is the means by which Americans express their opinions about their government. It provides Americans with the opportunity to affirm policies they like and change what they don't.

When our citizens vote, they not only elect their leaders, they choose a direction and set priorities for our nation.

Elections with integrity strengthen democracy. They confer legitimacy and boost public trust in government.

Concerns with earlier versions of voting and election systems led to the passage of the 2002 Help America Vote Act (HAVA). This Act requires the National Institute of Standards and Technology (NIST), over which we have jurisdiction, to work with the Election Assistance Commission (EAC) on technical, voluntary guidelines for voting.

Today we will discuss the current technical voluntary guidelines that are in place that for states to protect their voting and election systems.

Though these guidelines are voluntary, I hope to hear whether they are sufficient to safeguard our elections and whether states effectively use them.

This discussion is timely as many concerns have been raised in recent months about the vulnerabilities of electronic voting machines, voting over the Internet, and online voter registration.

In response to these concerns, our discussion today will review the security of the election system in its entirety.

We will examine what guidelines are in place, how we currently protect systems from potential technical vulnerabilities, and what kind of work – including research and development in my home state of Texas – is underway to protect future voting and election systems.

Last year, hackers from China infiltrated the Office of Personnel Management's database and stole confidential records and personal information on more than 22 million current and former federal employees, including those involved in our national security effort with the highest security clearances.

The attacks on voter registration databases in Illinois and Arizona are the latest instances of such attacks, this time with alleged ties to Russia. We have yet to take decisive steps to defend ourselves and deter attackers.

The President says we are more technologically advanced, both offensively and defensively, in cyberwarfare arena than our adversaries. So why won't he take the necessary steps to prevent cyber-attacks on our elections systems by foreign governments?

If we are attacked repeatedly and do nothing, we will have surrendered unilaterally and put at risk our economy, our national security, our very freedoms.

This Committee has held more than a half a dozen hearings on cybersecurity issues in this Congress. We know it isn't enough to respond to cyber-attacks with diplomatic protests.

We are going to hear from witnesses today about how the federal government can help states keep our election systems secure. But the single most important way to protect our election systems, to protect each American's right to vote and be heard, is for this administration – and for the next administration – to take decisive steps to deter and, if necessary, sanction foreign governments that attack us in cyber-space.

###