Statement of Chairman Lamar Smith (R-Texas)
A Review of Progress by the Department of Homeland Security (DHS), Science and Technology Directorate

Chairman Smith: Ongoing, productive research and development (R&D) is crucial to protect our country and its people.

Whether terrorists, cyber criminals, or drug or people smugglers, our adversaries are relentless and constantly adjust their tactics. In order to meet evolving risks and threats, we must continuously invest in R&D. Just as important, taxpayers' dollars committed to R&D must have a high return on investment.

Today, the Committee will continue its review of the Department of Homeland Security's Science and Technology Directorate and its important work.

In July 2014, the Committee held a hearing on technologies that would help secure our borders. Then in the following September, we held a joint subcommittee oversight hearing with the Homeland Security Committee.

The two witnesses at the September hearing were the Director of Homeland Security and Justice at the Government Accountability Office (GAO) and the Department of Homeland Security Undersecretary for Science and Technology, Dr. Reggie Brothers.

The witnesses and our Committee members focused on a series of GAO reviews that found serious problems with management and coordination of R&D within the Department of Homeland Security (DHS).

The GAO found the DHS's research and development efforts to be "fragmented and overlapping." GAO also found hundreds of millions of dollars spent in previous years on duplicative R&D projects by other offices within the Department.

GAO recommended that the Science and Technology Directorate develop stronger policies and guidance to define, oversee, coordinate and track R&D across the Department.

America's economy and security are threatened every day by cyber criminals and hackers. Unfriendly foreign governments launch regular cyber-attacks to undermine our national security and steal military and technological secrets.

Cyber-attacks against U.S. government and private sector networks continue to grow at an alarming rate. But with each new breach of private and public electronic networks, it's clear the full scope of the threat we face has yet to be realized.

At a subcommittee hearing last week, members of our Committee heard about the threat of cyber-attacks to the power grid. If just one major city were attacked in this way, the economic and societal consequences would be devastating.

The House Science Committee approved the only cyber legislation in the last Congress, the Cybersecurity Enhancement Act of 2014, which was signed into law.

Another area of particular concern is our government's failure to control our country's borders.

Unsecure physical and virtual borders threaten our national and economic security. A country that has lost control of its border has lost control of its future.

The magnitude of these and other homeland security challenges require constant advances to our technological capabilities. For instance:

- About 12 million containers arrive in the US every year which must be screened by DHS;
- More than two million passengers fly domestically every day who must be screened by the Transportation Security Administration;
- Nearly 100 million international air service passengers must be screened by Customs and the Border Patrol; and
- The annual number of land travelers to the United States who must be processed by our Border Patrol is approaching 250 million people.

There are not enough agents and screeners available to do this work. Instead, we must adapt, invent and, when necessary, create better technological solutions that are smarter, faster, less expensive, and more effective.

This morning, we will hear from Dr. Brothers on the progress made in the implementation of the GAO's recommendations. He also will update us on the S&T Directorate's initiatives to help DHS component agencies meet the full spectrum of threats.

<center>###</center>