



OPENING STATEMENT

September 17, 2015

MEDIA CONTACTS

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
House Homeland Security Committee**

Subcommittee Markup: H.R. 3490, H.R. 3493, H.R. 3510, and Committee Print

Remarks as Prepared

The Subcommittee meets today to markup several bipartisan pieces of legislation that would enhance the U.S. Department of Homeland Security's ability to carry out its mission and to protect the American people. Not only would these bills bolster DHS' efforts, they also provide increased accountability, transparency and oversight to ensure that Americans' taxpayer dollars are not wasted. In today's evolving threat environment that includes dynamic cyber threats, threats from ISIS, and a nuclear-armed Iran, DHS must have every tool at its disposal to keep the American people safe.

Today, we are considering a Committee Print of the DHS Science and Technology Reform and Improvement Act of 2015 to strengthen and improve the Science and Technology Directorate at DHS. In May, this Subcommittee held a hearing entitled, "Examining DHS Science and Technology Directorate's Engagement with Academia and Industry" to help further inform our efforts and this legislation. Threats and technologies are always changing. The DHS Science and Technology Directorate, or S&T, monitors those threats and utilizes technological advancements to develop and deliver solutions in order to prepare for future challenges and the critical needs of the DHS components. In light of DHS S&T's challenges, this legislation would make important improvements on how it conducts research and development. This legislation also defines a clear mission statement for DHS S&T and requires the Directorate to conduct portfolio reviews, a process that engages key leadership and stakeholders, to ensure research and development meets Directorate and Department goals and objectives.

Additionally, we will be considering H.R. 3490, the Strengthening State and Local Cyber Crime Fighting Act of 2015 to bolster State and local law enforcement efforts to fight cyber crime. This legislation would codify the National Computer Forensics Institute, or NCFI. The Institute was created in 2007 by the State of Alabama and is now operated by the United States Secret Service. Located in Hoover, Alabama, the NCFI is housed in a 32,000 square foot facility consisting of classrooms, mock courtrooms and an operational forensics laboratory. The NCFI has garnered a reputation as the premier cyber crime training center in the nation supporting State and local law enforcement investigators, prosecutors, and judicial officials. To date, the NCFI has trained and equipped more than 4,590 local officials from all 50 states and three U.S. Territories. These NCFI graduates represent more than 1,500 agencies nationwide.

Today's cyber criminals present a new challenge to our State and local law enforcement officers and judicial officials. Everyday cyber criminals' capability to carrying out devastating cyber attacks on Americans is growing. As such, it is imperative to support State and local law enforcement to protect the American people, small business owners from being exploited through their computers and mobile devices.

H.R. 3493, the Securing the Cities Act of 2015 offered by Mr. Donovan authorizes the Securing the Cities Program within the Domestic Nuclear Detection Office at DHS. The STC program develops, trains and equips State and local law enforcement to detect, prevent and mitigate a radiological or nuclear terrorist attack. The training and equipment provided to State and local law enforcement enables them to more effectively intercept radiological or nuclear material out of regulatory control. Terrorist groups such as ISIS and Al Qaeda have made their aspirations known to carry out WMD attacks against U.S. interests, and as such, it is vitally important that DHS is prepared to combat this threat. I would like to thank Mr. Donovan for sponsoring this legislation on this important issue.

Finally, I am happy to consider today the Department of Homeland Security Cybersecurity Strategy Act of 2015 sponsored by the Ranking Member from Louisiana, Mr. Richmond. This legislation would require DHS to develop and submit to Congress a cybersecurity strategy and implementation plan, as well as preclude any reorganization effort without Congressional approval to ensure proper oversight is conducted.

I would like to thank the Ranking Member for the work he and his staff have done to come together in a bipartisan way on these pieces of legislation. Each of them provides DHS with vital tools for protecting this country along with needed transparency and accountability of taxpayer dollars.

###