Statement of Rep. Ralph Abraham (R-La.)
H.R. 1224, the *NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017*

Rep. Abraham: Thank you Mr. Chairman.

H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017 is an extension of my ongoing interest over the state of our nation's cybersecurity.

Hardly a month goes by without some news of a cyber-attack leading to the successful breach of millions of Americans' financial, health, or other personal data.

During an informative Research and Technology Subcommittee hearing two weeks ago, a witness representing the U.S. Government Accountability Office (GAO) testified that "Cyber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, are evolving and becoming more sophisticated." The GAO witness also explained that "over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of February 2017, about 1,000 recommendations had not been implemented."

These are not pieces of information to be taken lightly. Last fall, this Committee marked up a bill I introduced that reflected a need for accountability, responsibility, and transparency by federal agencies relative to their cybersecurity capabilities.

The bill under discussion today takes the same general approach as last year's bill, which the Committee approved by voice vote. H.R. 1224 also reflects recommendations from two recent reports that were the focus of the Subcommittee hearing two weeks ago.

Highlights of the bill include:

- Amending NIST's mission to emphasize the principle that expanding cyber threats require the engineering of security from the beginning of a system's life cycle;

- Promoting federal implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework);

- Establishing a federal working group to develop quantifiable metrics to help federal agencies analyze and assess the effectiveness of the Framework in protecting their information and information systems;

- Directing NIST to complete an initial assessment of the cybersecurity preparedness of federal agencies;

- Directing NIST to initiate individual cybersecurity audits of each agency to assess the extent to which they are meeting the information security standards developed by the Institute; and

- Providing agencies and Congress with an audit report.

The Committee's jurisdiction over NIST provides it the ability to present the Institute with the flexibility to expand its functions in an effort to address the cybersecurity emergency facing our nation. It is to NIST's credit that the Committee regards the Institute as part of the solution, and not the problem. H.R. 1224 reflects the Committee's resolve to provide federal agencies all the tools it may be able to use to help remedy the federal government's cybersecurity shortcomings.

It is easy to sit back and state, with the benefit of NIST's reputation as an exemplary agency, that we should not consider changing the way the Institute operates because of what *might* happen or how the Institute's reputation or effectiveness *might* suffer.

But the current state of affairs do not suggest that the best way forward is to keep taking the path of least resistance. Much as the nature of cyber-attacks continue to evolve to reflect the sophistication of the cyber criminals, we in the government must also be willing to evolve to protect Americans and our government. That evolution starts with thinking outside the box instead of maintaining a business as usual approach.

H.R. 1224 establishes the Committee's mark on a very important issue. It sets the tone for future cybersecurity discussions by taking some first steps to strengthen federal cybersecurity defenses, and holding federal agencies accountable through regular cyber audits.

I urge my colleagues to support this bill, and I yield back.

###