

Opening Statement  
**Ranking Member Eddie Bernice Johnson (D-TX)**

House Science, Space, and Technology Committee  
Markup of: H.R. \_\_\_\_\_, the  
*“NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017”*  
March 1, 2017

Thank you Chairman Smith.

I understand and sympathize with the Chairman’s desire to move cybersecurity legislation. Cybersecurity is a critically important topic, and one that invites significant press attention. We had a good hearing before the Research & Technology Subcommittee just two weeks ago, during which we heard many good recommendations from widely respected experts. Some of those recommendations fell within our Committee’s jurisdiction, others did not.

I do remember the panel unanimously praising NIST’s role in cybersecurity. I also remember discussion about developing metrics for the adoption of NIST’s Cybersecurity Framework. Witnesses also discussed requiring Federal agencies to incorporate the Framework into their information security programs.

I can see where Mr. Abraham has attempted to incorporate some aspects of those recommendations into his legislation. However, I specifically recall GAO’s recommendation that the Department of Homeland Security, and not NIST, carry out surveys and assessments of the adoption and effectiveness of the Cybersecurity Framework. NIST itself has steadfastly maintained that they are the wrong agency to do it, and not just because of limited resources.

I do not remember a single witness, or a single expert recommendation suggesting that OSTP should be given any role in evaluation or oversight of cybersecurity in the private sector or the Federal government. Perhaps if we substituted OMB or DHS for OSTP everywhere in this bill, it might make more sense. The Majority has inserted an entirely new agency into a policy matter in which they have no expertise and no business being a part of. In doing so, the bill also duplicates authorities and responsibilities clearly assigned to OMB and DHS in current law.

Finally, and speaking to what may be the strangest part of this bill, I do not remember any expert ever recommending that NIST be given the responsibility to conduct annual cybersecurity audits of other agencies. NIST is not an auditing agency.

They have no such history, expertise, or capacity. They are a standards and technology agency. In addition, a single FISMA audit costs between a few hundred thousand to a couple of million dollars, depending on the size and mission of the agency. Nowhere in this bill do we provide NIST with the tens of millions of dollars of additional funding to become the cybersecurity auditing agency of the Federal government. This is a massive unfunded mandate levied on an agency which is already over tasked. Moreover, current law already assigns this very responsibility to agency inspectors general. And no expert I know of has questioned the quality or integrity of the IGs' work. In fact, IGs know and understand their own agencies' business operations and information systems infrastructure better than NIST ever will. In short, I remain thoroughly baffled by this proposal in the legislation before us today.

Mr. Chairman, I've said this before, and I will say it again here. I stand ready to collaborate and cooperate with you on cybersecurity legislation and oversight. We've been able to do so in the past, including for the Cybersecurity Enhancement Act of 2014. However, the bill before us today has a number of controversial new elements which were clearly not vetted with the cybersecurity community or the Administration. I will not support passage today of legislation which will undermine the very agency we are tasking with keeping our cyber infrastructure secure.

I would hope that after this markup, the Majority will take the time to address the concerns that have already been raised in the short time this bill has been publicly available.

I yield back.