Statement from Vice Chairman Frank Lucas (R-Okla.)
Markup of H.R. 6229

Vice Chairman Lucas: Thank you Mr. Chairman for the opportunity to speak on behalf of my bill, H.R. 6229, the National Institute of Standards and Technology (NIST) Reauthorization Act of 2018.

NIST works to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology. This legislation authorizes NIST's Industrial Technology Services account, construction accounts, and bolsters the Scientific and Technical Research and Services lab account for fiscal years 2018 and 2019.

NIST has the mission and capabilities to contribute to areas critical to the United States' global competitiveness. To this end, for fiscal year 2019, this legislation authorizes increased investments in four emerging technology areas: quantum science, artificial intelligence and data science, advanced communications and the internet of things and composites research and standards development.

As we've just heard during our consideration of the *National Quantum Initiative Act of 2018*, an international race to claim quantum supremacy has begun. And it is not just in quantum that we are racing our international rivals to develop. By facilitating NIST's development of tools to address performance and reliability concerns of artificial intelligence (AI), NIST will accelerate the implementation of AI systems and give U.S. industries a competitive edge.

The discoveries and technological advances that will stem from these investments will significantly affect the nation's economy in the coming decades.

One of the great challenges of the 21st Century is cybersecurity. This legislation helps NIST address the growing cybersecurity threat landscape by providing for the increase of its fundamental and applied cybersecurity research to address key questions relating to the measurement of privacy, security and the vulnerability of software tools and communication networks.

This committee has held multiple hearings on cybersecurity since the news that the Office of Personnel Management (OPM) was the target of two massive data

breaches—exposing the sensitive information of over 21 million Americans, including me and many of my constituents.

Last month the Office of Management and Budget (OMB) published its "Federal Cybersecurity Risk Determination Report and Action Plan" in accordance with Trump Executive Order 13800. The report identifies that 74 percent of federal agencies participating in the risk assessment process have cybersecurity programs that are either at risk or high risk. The report also confirms the need to take bold approaches to improve federal cybersecurity.

NIST plays a very important role in protecting from cyber threats through its ongoing cybersecurity research, including the applications of blockchain technology, and by providing guidelines and standards to help reduce cyber risks in federal agencies and critical infrastructure. This legislation requires NIST to enhance and expand its guidance and assistance to Federal Agencies to help them to effectively use the NIST-authored "Framework for Improving Critical Infrastructure Cybersecurity."

The President's Executive Order directed each agency to use the framework. It is my hope that this language will prompt agencies to rely on NIST's expertise in order to adopt these best risk management practices within their agencies.

This committee has a long, bipartisan record of support for NIST and its contributions to research and development. It is my hope that all of my colleagues on the committee will continue that tradition and support this bill. Thank you again Mr. Chairman for bringing this important piece of legislation up for consideration, and thank you to Ranking Member Johnson, Ranking Member Lipinski and the many other members of this committee for working with me and supporting this bill. I yield back the balance of my time.

###