Opening Statement of Ranking Member Cedric L. Richmond (D-LA)

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Joint Hearing: "Enhancing Preparedness and Response Capabilities to Address Cyber Threats"

May 24, 2016

In developing policy and budgeting for cyber preparedness and response, it is crucial we know what needs protecting, how badly protection is needed, and what kinds of redundancies can be made available.

For critical infrastructure entities, after knowing what machines are operating on a network, what applications they are running, and what privileges have been established, the posture of cybersecurity for each of these entities and systems networks is key.

Also, for critical infrastructure enterprises and supply chains, the advent of, 'bring your own devices', along with the growing sophistication of smart phones and tablets involved in day-to-day infrastructure operations, compounds cybersecurity efforts and increases our resiliency challenges.

Knowing where to devote efforts to protect our information security in critical infrastructure organizations is a core choice, particularly in determining how much defense to commit to the perimeter, and how much to commit to internal threats.

Consider the potential for adversaries to employ countermeasures…as defenses are installed on our systems, we must acknowledge that we are dealing with a thinking and competitive opponent in the cyber world…and that as we install measures to thwart hackers that very act tends to induce countermeasures from our foes, as hackers probe for ways around or through our new defenses.

As new versions of cyberattacks emerge affecting critical infrastructure, it will be important to have the DHS Industrial Control Systems Computer Emergency Response Teams, or ICS-CERT, and the Joint Interagency Task Force consisting of the National Institute of Standards and Technology, or NIST, the Department of Defense, and the Intelligence Community, clearly delineate and prioritize their roles in protecting critical infrastructure, and to have that as well-defined as possible.

A good place to start is to build a body of cyber knowledge on how various critical infrastructure cyber systems are likely to fail, which is a necessary prerequisite to preventing failure, and then share that information among all sectors.

Most experts tell us this is a daunting proposition, in light of the fast pace and range of cyber threat vectors that present themselves daily, but we must try.

In closing, any critical infrastructure sector that is prepared to share what went wrong and what could be done better next time, will create the most likely scenario to produce higher levels of cybersecurity and resiliency for future regional and national cyber-emergency situations.