Opening Statement of Ranking Member Cedric L. Richmond

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"Emerging Cyber Threats to the United States"

February 25, 2016

The Department of Homeland Security plays a fundamental role in the national effort to increase our collective cybersecurity, but it cannot achieve its mission without a foundation of voluntary partnerships with the critical infrastructure community, the information security industry, and our government partners.

The privately-owned critical infrastructures that are everywhere in my district, including—ports, energy and pipeline networks, chemical manufacturers, and refineries— ship and supply goods and raw materials to all parts of our country, and are vital to the jobs and economic well-being of my part of the world.

When the cyber information security and network systems fail for these kinds of sites, whether from a natural disaster or a man-made intrusion, everyone feels it. It is in the national interest to safeguard such critical infrastructure, and to make sure there are adequate protections from cyber and information and data interruptions.

This Subcommittee has oversight responsibilities for the Department's US-CERT and ICS-CERT teams that provide the foundation of the U.S. government's approach to securing and safeguarding the resilience of civilian cyber, and critical infrastructure essential services. It will be necessary for this Subcommittee to continue to do all we can to help DHS develop a workable, national cyber protection strategy and framework for critical infrastructure entities, and small and large businesses, in order to protect our economy.

After this Subcommittee and Full Committee passed important information-sharing legislation last year, that legislation found its way to the President's desk where he signed the Cybersecurity Information Sharing Act, or CISA, on December 18th, of 2015.

Today I hope to hear from our witnesses how the Department is doing with its new information-sharing authorities and challenges, and how cyber and information security industries are expanding their collaboration with the Department as a result of the legislation.

It will be important to know how cybersecurity companies can continue to collaborate with the Department to help US-CERT and ICS-CERT serve as the center of our national integration, information sharing and collaborative analysis, for domestic and global cyber threat intelligence.

Finally, I hope to find out from our witnesses how we can help further the ability of the DHS's National Cybersecurity and Communications Integration Center, or NCCIC, to receive and analyze information at machine speed—an essential component of getting a leg-up on the ever changing landscape of worldwide cyber threat intelligence.