Opening Statement of Ranking Member Cedric L. Richmond

Subcommittee on Cybersecurity, Infrastructure Protection, and Security

"Value of DHS' Vulnerability Assessments in Protecting our Nation's Critical Infrastructure"

Tuesday, July 12, 2016

Whether it's going about our daily lives, running a business, or a local government, we all rely on the security and resiliency of our critical infrastructure. As we have seen after disasters like Katrina, Rita, Sandy, or the recent devastation in West Virginia, the ability to recover quickly is crucial.

In my district, as in many districts across the country, multiple DHS components, and a range of other agencies conduct vulnerability assessments—the Coast Guard in the ports in my district, the TSA in airports and for pipelines and transportation corridors, and DOE and FERC for electric grid vulnerabilities.

Risk assessment involves integrating threats, vulnerabilities, and consequence information, and then deciding which protective measures to take based on an agreed-upon risk reduction and recovery strategy.

Within DHS, the National Infrastructure Protection Plan outlines how government and the privately-owned critical infrastructure community can work together to manage risks and achieve physical and cyber security and resiliency.

It is important to remember that these are voluntary, non-regulatory assessments, and they represent the foundation of the NIPP risk-based programs designed to prevent, deter, and mitigate the risk of a terrorist attack, or natural disaster.

The DHS Protective Security Advisors, and Cybersecurity Advisors, conduct these assessments and focus on coordination, training, and building existing relationships with state, local, tribal, territorial, and private sector partners.

This year, President Obama requested additional funds to expand the PSA and the CSA programs, in hopes of melding physical security with cyber security, and in line with the Secretary's DHS Unity of Effort initiative.

Critical infrastructure vulnerability assessments present DHS and the current NPPD Directorate with one of their most complex challenges and, as GAO has suggested in their testimony, it is not clear that the Directorate has had a consistent and systematic approach for identifying nationally critical assets, assessing the risks they pose, and using that information for cost-effective allocation of resources.