Opening Statement of Ranking Member Donald M. Payne, Jr. (D-NJ)

Subcommittee on Emergency Preparedness, Response, and Communications

Joint Hearing: "Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management"

311 Cannon House Office Building - October 30, 2013

Yesterday marked the one year anniversary of Super Storm Sandy, which devastated communities all along the East Coast, and especially in my home state of New Jersey. Although the people of New Jersey – with a lot of help from the Federal government - have begun the long effort to rebuild what was lost, much work remains.

I know I am not alone when I say that the people affected by Hurricane Sandy can be sure that Members of this panel will continue to work to make sure that the communities are rebuilt and the lessons learned are incorporated into future disaster plans.

With that, I will turn to the topic of today's hearing: responding to a cyber attack. Last month, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing reviewing the findings of the Federal Emergency Management Agency's 2013 National Preparedness Report. For the second year in a row, States indicated that – of the 31 core capabilities – cybersecurity is one of the capabilities about which they are least confident.

The threats posed by a cyber attack are not new. But the impact of a cyber attack becomes more grave as every aspect of government and the private sector become more reliant on cyber technologies. For example, communications essential to an effective emergency response, from the Emergency Alert System, to E9-1-1, and eventually FirstNet, are all vulnerable to a cyber attack.

The data networks and computer systems used to coordinate an efficient response and ensure that adequate resources are deployed to the appropriate location are similarly vulnerable to a cyber breach. A cyber attack on any of these systems could severely undercut Federal, State, and local abilities to respond to disasters effectively.

Moreover, we have seen a significant increase in cyber threats to our critical infrastructure. We know that disasters like Super Storm Sandy can wreak havoc on our power systems but we rarely consider the harm that a malicious cyber attack could do to our electric grid.

Accordingly, I have introduced the SMART Grid Act, which would provide for a comprehensive assessment of actions necessary to expand and strengthen the capabilities of the electrical power system to prepare for, respond to, mitigate, and recover from a natural disaster or cyber attack to the electric grid.

My legislation will go a long way to provide sector-specific awareness of cyber vulnerabilities and how to address them. We must help State governments undertake similar efforts to understand the cyber threats posed to their networks and how to address them. It is no secret that a lack of funding has contributed to the lack of confidence states have in their cybersecurity capabilities.

I will be interested in learning how cuts to Homeland Security Grant funding since 2011 have affected State cybersecurity efforts. I have also heard that States have struggled to implement a governance structure for cybersecurity and that finding a workforce with the appropriate training has proven difficult.

So I will be interested to learn how the Department of Homeland Security is helping States identify best practices for an effective cybersecurity governance structure and improve training for State cybersecurity workforces. And I look forward to learning more about how State Emergency Managers are working with State Chief Information Officers to understand the role each play in responding to a cyber incident.