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

Joint hearing: ENHANCING PREPAREDNESS AND RESPONSE CAPABILITIES TO ADDRESS CYBER THREATS

Emergency Preparedness, Response and Communications

Tuesday, May 24, 2016

The last time our Subcommittees held a joint hearing on this subject was during the 113th Congress – about three years ago. What we learned is that cyber threats are the new frontier of disaster response.

Our legacy response doctrine – from the National Response Framework to the *Stafford Act* – are rooted in an era that pre-dates reliance on cyber networks and growing threats posed by sophisticated hackers. Despite our best efforts to ensure that our national preparedness doctrine is responsive to evolving threats, it has not kept pace with cyber threats.

My district is rich with critical infrastructure, all of which rely on cyber networks. Within two miles, we have major transit systems, chemical facilities, and refineries mixed among homes, schools, and hospitals.
A hack of any one of these targets could have devastating cascading effects and could risk overwhelming our brave first responders.

And we know the threat is real. Earlier this year, Iranian hackers breached the Bowman Avenue Dam network in Rye, New York. Fortunately, the dam was offline for repair when the authorities discovered the breach. But I am worried it is only a matter of time before the hackers are successful – and we need to be prepared when they are.

I applaud efforts at the State level to confront the cyber threat head on. Some States – like California and my home state of New Jersey – have established State-level cyber information-sharing centers modeled after the National Cybersecurity and Communications Integration Center. I will be interested to learn whether these centers facilitate improved information-sharing and encourage better relationships among non-traditional partners who would play important roles in a cyber response.

At the same time, I would be remiss if I did not note that while States annually indicate that they lack confidence in their cybersecurity capabilities in the *National Preparedness Report*, very few invest Homeland Security Grant funding to address that capability gap.

I will be interested in understanding why – is it because the Federal government has not provided adequate guidance on how to address the threat or whether the amount of grant funds available after cuts to grant programs in recent years prevents States from investing in cyber capabilities.

While I am on the subject of grant funds, I have been outspoken about my opposition to the proposed cuts to the Homeland Security Grant Program as well as the Port and Transit Security Grants. I have serious concerns that the proposed cuts would only further jeopardize whatever progress States and other grantees are making to address cyber threats, and I will be interested in the witness' thoughts on that point.

Finally, as I indicated, our Subcommittees held a joint hearing on responding to a cyber attack about three years ago. The witnesses at that hearing made two points that stuck with me.

First, the witnesses emphasized that a response to a cyber attack will require people – from chief information officers to emergency manager to private sector partners – to break out of their silos and coordinate with non-traditional partners. Second, they said that existing disaster response guidance does not adequately address the complexities of responding to a cyber event.

I look forward to hearing our witness' opinions on how the National Incident Management System, the National Response Framework, and other disaster management doctrine should be updated to reflect the unique qualities of a cyber event.