Opening Statement of Rep. Bonnie Watson Coleman

"Defense Support of Civil Authorities: A Vital Resource in the Nation's Homeland Security Missions"

Subcommittee on Emergency Preparedness, Response, and Communications

Wednesday, June 10, 2015 at 10:00 AM

The capabilities of our defense resources are vast and diverse. Though ordinarily jurisdictions may not look to partnering with National Guard or the Defense Department, the boots on the ground and capacity that they can supply are a great multiplier. Just last month, units from the Texas and Oklahoma National Guards provided surge capacity to State and local responders during and after massive floods pummeled the region.

With the upcoming ten-year anniversary of Hurricane Katrina and three-year anniversary of Super Storm Sandy, we are reminded once again of the important role that defense resources play in response and recovery. Although many important reforms to facilitate improved integration of defense assets into civil response plans were implemented between Hurricane Katrina and Super Storm Sandy, every after action report identified improvements that must be made.

From clarifying the role of the dual-status commander to improving training to ensure that command and control structures are well-exercised, there is more work to be done to drive efforts for better coordination on the ground, particularly during complex multi-state catastrophes. The testimony prepared by Mr. Kirschbaum underscores my point. Madam Chair, today's hearing could not come at more appropriate time.

As a Subcommittee, we have expended significant time on exploring response challenges associated with chemical and biological threats. In the event of a catastrophic chemical or biological incident, we know that defense resources are an integral part of an effective response. Today's hearing affords the Subcommittee the opportunity to deepen our understanding of how defense resources support our Nation's chem-bio response capabilities.

Another area of great interest to Members on both sides of the aisle is the Nation's response capability when it comes to another emerging threat area--- cybersecurity. The disclosure last week by the Department of Homeland Security and Office of Personnel Management that the personnel files for approximately 4 million current and former Federal employees were hacked brings this threat into real focus. The challenge of securing our nation's cyber infrastructure and networks demands an all-hands-approach.

DHS has a dual-cyber role: It is responsible for helping to protect Federal networks and partnering with critical infrastructure owners and others in the private sector to bolster cybersecurity. In the event of a major cyber incident which results in cascading failures of multiple interdependent, critical, life-sustaining infrastructure sectors, an effective and timely civilian response will necessarily depend on coordination with defense resources. Recent announcements by the National Guard Bureau of the creation of Cyber Protection Teams is a welcome development and reflects an awareness of the likelihood that civilian authorities will look to the Guard for such support.

These Cyber Protection Teams will train and operate on a traditional part-time basis in support of their respective state National Guards. But when activated for Federal active duty, the teams will provide surge support to Army Cyber Command and support defensive cyberspace operations. I will be interested in learning more about how this cyber capability will coordinate with and complement the civilian response capability.

Along those lines, I would like to thank Mr. Gaynor, the Director of the Rhode Island Emergency Management Agency, for being here today to talk to us about how the State leverages defense assets in its cyber response plans. Although I am encouraged to learn that cyber response coordination is underway, I was concerned to learn in GAO's written testimony that the Department of Defense has not yet adequately aligned its guidance on preparing for and responding to domestic cyber incidents with national-level guidance. I hope we can learn more about DoD's progress in that regard today.