



## HOMELAND SECURITY COMMITTEE

### **Statement of Subcommittee Chairman Dan Donovan (R-NY) Emergency Preparedness, Response, and Communication Subcommittee Homeland Security Committee**

*Joint Hearing: "Enhancing Preparedness and Response Capabilities to Address Cyber Threats"  
May 24, 2016*

#### Remarks as Prepared

First, I'd like to thank Chairman Ratcliffe and Ranking Member Richmond for working with me and Ranking Member Payne on this issue. Also, I would like to thank all the witnesses for coming today to join in this important discussion.

As we are all aware, the cyber threat is real from both state and non-state actors. The countless cyber-attacks against the United States and its citizens, including major attacks against Target, Home Depot, OPM, and Anthem, are just the tip of the iceberg. I believe that the number and magnitude of attacks will only increase, especially as more and more of our lives become connected to the Internet. It is imperative that we ensure that our State and local officials as well as our first responders are prepared to protect against and respond to a cyber attack.

Furthermore, we are seeing an increase in the number of cyber attacks that if successful can cause widespread physical damages to a community and require a whole of community response. Already, state and non-state actors have attempted to interfere with 911 call centers, send out inaccurate alerts and warnings, and tried to take over the controls of a dam. While we have taken numerous steps to enhance our capabilities, we have a long way to go in addressing these threats.

As a Member of Chairman Ratcliffe's Subcommittee, I have heard about the progress the Federal government, States, and localities have made in enhancing our cybersecurity capabilities, but I'm left scratching my head when I see for the fourth year in a row, the National Preparedness Report, released by FEMA, indicates that States continue to report cybersecurity as the lowest core capability. What is preventing us from reaching the appropriate level of cybersecurity? What obstacles are States facing and what can we do to help?

I'm especially interested in learning more about what happens after a cyber attack that has physical consequences. Who is in charge of the response and how are first responders coordinating with cyber officials who are trying to mitigate the attack? I know States like California have set up task forces to answer these exact questions.

Additionally, in 2012, the National Level Exercise looked at the Nation's ability to respond to a large-scale cyber attack with physical consequences. One of the key recommendations from this exercise was to finalize a cyber response plan that clearly defines the roles and responsibilities of all the potential response entities.

Four years since the exercise and six years since the interim draft of the National Cyber Incident Response Plan (NCIRP) was released, we still do not have a finalized and approved NCIRP. Developing and finalizing this plan needs to be a priority of the Federal government. I understand that the Department plans to finally begin stakeholder engagement on the development of the final plan in the coming weeks. I certainly hope they will be engaging with all of the witnesses at today's hearing to get their feedback.

Also, I have heard that while sharing cyber information is becoming more prevalent, there is still confusion on who States should talk to when an incident occurs and the sharing of cyber related information with the emergency management and first responder communities is ad hoc at best.

These people are going to be the first on the scene and should have insight into whether the incident they are responding to has been caused by a cyber attack. Can States utilize their fusion centers to be a force multiplier to disseminate critical cyber information? I know my State is taking this approach and I'm interested to hear if it has been successful.

A few years ago, Secretary Johnson made a statement that I feel is still true today. He said "[c]ybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we are. We are all connected online and a vulnerability in one place can cause a problem in many other places. So everyone needs to work on this: government officials and business leaders, security professionals and utility owners and operators." And that is why we are here today.

I want to thank all the witnesses for testifying today and I look forward to highlighting the good work you all are doing to enhance your cybersecurity capabilities and learning about what areas are still a challenge and how the Federal Government can help in mitigating those gaps.

###