



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

October 30, 2013

Media Contact: Charlotte Sellmyer
(202) 226-8417

**Statement of Subcommittee Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
Committee on Homeland Security**

Joint Subcommittee Hearing:

**“Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency
Management”**

Remarks as Prepared

Thank you Chairman Brooks, Ranking Member Payne, and Ranking Member Clarke for convening today’s hearing.

Our committee is coming together at a time when the threat of a cyber attack on our nation is escalating. Our nation’s top national security and cybersecurity experts continually point out that it is a question of when, not if we will be attacked. Over the past year the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee has looked at multiple ways that our nation’s critical infrastructure remains vulnerable to an attack.

Today, the cyber threat comes from a variety of actors, including nation states, criminal organizations, and individual hackers. In March, our subcommittee held a hearing on these threats, particularly those posed by China, Iran, Russia, and North Korea. We also looked at the crucial aspect of protecting Americans’ privacy in an April hearing. In addition, our subcommittee has been working to provide proper oversight on the President’s cybersecurity Executive Order, and the capabilities and responsibilities given to the Department of Homeland Security to oversee cyber threat information-sharing, and protection of chemical facilities.

Today's hearing is the logical next step in our oversight capacity. Joining together with the Subcommittee on Emergency Preparedness, Response, and Communications we will examine the Department's readiness to work with its state and local partners to respond to a disabling cyber attack.

Our nation must be prepared should an event wipe out crucial portions of our power grids. Prevention is not enough; FEMA must have the capabilities to respond with action. Moreover, state and local public health and safety entities need to be at the forefront of incident response. That is why today's hearing is so important.

In its 2012 National Preparedness Report, FEMA found that cybersecurity ranked last in states preparedness capabilities. The report states that, "Cybersecurity was the single core capability where states had made the least amount of overall progress, with an average capability of 42 per cent."

In its 2013 report, FEMA noted gains, but states continued to rank cybersecurity as their weakest core capability. In fact, FEMA found that only 24 per cent of state chief information security officers were confident in their state's ability to protect against cyber threats. That is an unacceptable level of readiness. I stand with Members of this committee on both sides of the aisle determined to work with DHS and state and local governments to improve this.

Chairman McCaul and I have spent the year working with key stakeholders to address major gaps in critical infrastructure protection. We have released draft legislation of the National Cybersecurity and Critical Infrastructure Protection Act of 2013, which among other things will authorize DHS' Cyber Incident Response Teams to provide technical assistance and crisis management to state and local security preparation and response units.

Additionally, our legislation will help to improve participation and increase the sophistication of threat analysis at the National Cybersecurity and Communications Integration Center (NCCIC), as well as at the Multi-State Information Sharing and Analysis Center (MS-ISAC) in Albany. The MS-ISAC was created so the federal government can share cyber threat information with the states.

I look forward to hearing from our panel of experts today, and to continue working with the committee and the Administration to combat the threat of cyber attacks.

###