



HOMELAND SECURITY COMMITTEE

Statement of Subcommittee Chairman John Ratcliffe (R-TX) Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee

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

Remarks as Prepared

Good morning, I want to thank Chairman Donovan and Ranking Member Payne for working with myself and Ranking Member Richmond on this issue. I also want to thank the witnesses for coming today to speak on this important topic. On the Cybersecurity, Infrastructure Protection and Security Technology Subcommittee, which I chair, we often discuss the wide variety and high number of cyber threats that are out there and growing. Today, we are going to hear about the other part of the equation, which is the people, the hours, and programs designed and dedicated to preparing for and responding to the dangers that these cyber threats pose.

Hopefully having this discussion at a national level will help bring to light some of the best practices and most evident areas for improvement that will be applicable to every level of government whether it be at the Federal, State, or local level. Because the truth is, every level of government is constantly having to face and respond to these threats. We all need to work together to understand the tactics, techniques and procedures of hackers in order to better equip ourselves and face the threats of tomorrow.

It is important that we spend as much time and energy thinking about the solutions that secure Americans as we do on the examination of the dangers. The purpose of today's hearing is to focus on seeking those solutions to make America safer. In that spirit, we are constantly seeking to improve upon and expand the programs and partnerships with both the private sector and State and local governments that function to make Americans safe. These partnerships are the nuts and bolts to secure Americans against the havoc that is possible should a bad actor successfully disrupt or damage one of the many systems that we rely on for everyday life such as our water and our power.

What we are hoping to gain from today's hearing is what more we can be doing to further these partnerships and programs. The importance of the flow of information cannot be stressed enough as information is the currency with which security and insecurity is established in today's age. As fast as the bad actors are moving in cyberspace, we have to be constantly moving faster to stay ahead of them. While they only have to be right once to do damage, we must be resilient and stand perpetually ready with a plan and with answers.

I'm glad to be having this joint hearing to highlight the interconnectedness of the response plans that are in place in the case of a devastating cyber event, and the first responders who carry them out. At the federal level we have the ability to push out and develop plans beyond the capability currently available to states, but it is the responders already in the area who will be the first people that those most directly affected will see when a catastrophic cyber attack occurs.

As Mr. Donovan mentioned, the draft National Incident Response Plan or NCIRP (N-Chirp) was delivered to the Whitehouse in the fall of 2009. In March of 2010, a draft interim was released but not approved, subject to ongoing review by the administration. It has now been 6 years since the release of the interim draft, with stakeholder engagement just now starting. While 6 years is entirely too long for any type of response plan to sit on a shelf in the Whitehouse, it is especially dangerous in the case of cyber. In 2014, Congress passed a law to require this cyber incident response plan to be finalized. Clearly, this administration, by not finalizing this plan, does not take cyber incident response planning seriously. It begs the very obvious question "What if there is a significant cyber attack in the U.S.? Does every level of government know their role and how cyber response will be coordinated?" We are neither too ignorant nor too proud to think that a major cyber incident is outside of the realm of possibility so I would like to take this moment to convey that we are watching the development of this document very closely.

It is very apparent that we have a lot more work to do. Securing our States from cyber threats now includes entirely new roles and responsibilities that didn't exist 50 years ago. Discussing, examining, and encouraging the programs and partnerships that Americans rely on is absolutely crucial in guaranteeing the solvency of our ways of life. I look forward to hearing from the witnesses to learn what more can and should be done to advance the security of the American people.

###