



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

Homeland Security Committee

*Cyber Preparedness and Response at the Local Level
April 7, 2016*

Remarks as Prepared

Cyber threats are exponentially increasing. They come from criminal organizations; nation states like China, Russia, and Iran; and even terrorist groups like ISIS.

These attackers don't only target federal networks, big banks, and national retail chains. They also hit towns, families, and local businesses.

So there is a great need to address cybersecurity at the state and local level. From emergency response centers, Department of Motor Vehicle Offices, to courthouses and to our critical infrastructure, the exploitable vulnerabilities and possible consequences for public safety are alarming.

On the law enforcement side, FBI Director James Comey recently testified that "An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated."

It's incredible that federal law enforcement is seeing a cyber element to almost every crime. And because society is increasingly connected, we can be certain state and local law enforcement are seeing the same trend—arguably with fewer tools to address it.

It no longer takes a sophisticated cyber criminal to compromise sensitive information from companies and everyday Americans, and law enforcement is seeing a cyber element to almost every crime.

It is vital that state and local law enforcement, prosecutors and judges be properly trained to respond to cyber crime and protect the American people.

We've recently seen a flurry of "ransomware" attacks against hospitals—at least one located here in Texas Fourth District—where patients' personal medical data is encrypted and held hostage until the hospital pays a "ransom" to get it back.

And reports indicate that cyber attacks against emergency workers are spiking and will continue to rise.

We all recognize that interconnectivity and automation increase convenience and improve responses. Emergency services are just one area where automation and interconnectivity provide clear benefits. But while these technologies increase efficiency and cut costs, they present new risks that—if exploited—could bring vital emergency services and our critical infrastructure to a halt.

Regardless of the magnitude of a natural or man-made disaster, first responders—firemen, police, paramedics, and National Guardsmen—are the ones on the scene. Their ability to communicate and execute key command and control responsibilities during an incident often depends entirely on Internet-enabled technologies.

As we examine cyber preparedness and response at the state and local level, I'm pleased that we're joined by a number of distinguished witnesses who are at the tip of the spear in this effort. I look forward to hearing about how they're preparing for, responding to, mitigating and investigating threats in cyberspace.

I'm also pleased that this hearing is taking place, not in the Halls of Congress, but right here in the Fourth District of Texas—the first ever congressional hearing in Grayson County.

Police, prosecutors, judges, paramedics, and firefighters need appropriate tools and training to respond to increasing threats. And to make sure they are fully equipped, we must hear directly from them.

The best solutions, believe it or not, don't usually come from Washington, DC. People often hear me say that governing is a team sport, and I think that today's hearing, and the location of today's hearing, reinforces that.

As Chairman of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, I have been closely examining these challenges. I will continue to lead efforts in Congress to strengthen our nation's cyber defenses and provide for the common defense against these national security threats.

Last fall I authored and moved legislation to strengthen state and local cyber crime fighting efforts. Specifically, the legislation would support the National Computer Forensics Institute, or NCFI, run by the U.S. Secret Service that provides greatly-needed cyber forensics training to state and local law enforcement across the country, including to those right here in Texas' 4th district. We are pleased to be joined by former Greenville Detective, Don Waddle, who was trained by the NCFI.

Today, I hope this Subcommittee will learn how first responders are being trained to address cyber incidents, how first responders are preparing for and responding to cyber incidents, and how local law enforcement officials are being trained in computer forensics.

This hearing will provide needed background to further this Subcommittee's efforts regarding cyber training and workforce needs at the state and local level. Cybersecurity is a shared responsibility involving all levels of government and the private sector. While much has been done to improve the nation's cybersecurity, a number of challenges remain. I look forward to hearing from our witnesses today as we consider ways to address those challenges.

###