



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

*Opening Statement*

November 21, 2014

**Media Contact:** Lauren Claffey, April Ward  
(202) 226-8477

---

**Statement of Subcommittee Chairman Jeff Duncan (R-SC)  
Subcommittee on Oversight and Management Efficiency  
Committee on Homeland Security**

**“Emergency Preparedness: Are We Ready For A 21st Century Hugo?”**

**Remarks as Prepared**

September 21st marked the twenty-fifth anniversary of Hurricane Hugo—the most devastating disaster to affect South Carolina in the past century. The storm hit the low country with an unprecedented ferocity. It was responsible for 49 deaths, the equivalent of over \$13 billion dollars in damage in 2014 dollars, and displacing 60,000 from their homes. Hugo required a major response, for which South Carolina was unprepared. However, the ordered evacuation of 250,000 would pale in comparison to what would be needed today. Over a million now live in the area Hugo threatened.

Fortunately, South Carolina state and local first responders are better prepared and equipped to handle a variety of emergencies today. For example, just last month, the South Carolina Emergency Management Division organized a major drill to prepare for the threat of earthquakes in the state. Over 277,500 signed up to participate in the Great Southeast ShakeOut earthquake drill. Such events are an important way for our citizens to become better prepared and develop plans needed to respond to potential disasters.

Major General Robert Livingston—who we are honored to have as a witness at our hearing—has said that South Carolina’s National Guard has much more advanced tools at its disposal to respond than when Hugo made landfall. Specifically, the Guard has increased aviation assets and engineering capabilities. South Carolina’s Emergency Management Division has also increased its planning efforts to be more proactive than we were in the days of Hugo.

However, our first responders face an array of new threats today. The days of only preparing for natural disasters like hurricanes, floods, and earthquakes are behind us. Most recently, we’ve seen disturbing images from Texas of local law enforcement quarantining homes to prevent the spread of Ebola. The Administration’s failure to effectively stop the spread of Ebola to the US has put significant pressure on

state and local responders to ensure they have plans and training in place to deal with possible public health emergencies. Yet even the Department of Homeland Security—the agency responsible for screening foreign travelers entering the US—has failed to effectively manage pandemic preparedness supplies for its workforce, such as personal protective equipment and antiviral medical countermeasures according to a recent Inspector General report. The Federal government’s ineptitude has shown that our state and local first responders must be prepared to handle threats even half a world away, like Ebola.

In addition to living in a world where foreign viruses are only a flight away, we are increasingly interconnected through the Internet. The Director of the FBI, James Comey, recently called the cyber threats facing our nation “an evil layer cake” of nation state actors, organized cyber syndicates, hacktivists, criminals, and pedophiles. How does this involve emergency preparedness? As the number of cyber-attacks impacting Americans increase, federal, state, and local officials need to be prepared to respond to the virtual aftershocks that follow.

These cyber threats don’t simply threaten businesses and individuals that use the internet. When increasingly everything is connected to information systems and the Internet, even the protection of facilities is at risk to cyber-attacks. Specifically, facilities contain building and access control systems, such as heating, ventilation, and air conditioning; electronic card readers; and closed circuit camera systems could become vulnerable due to their connectivity to other networks and the Internet. For example, in 2009, a Dallas-area hospital security guard loaded a malicious program into the hospital’s system. Court records showed that this breach could have affected patients’ medications and treatments. The Department of Homeland Security (DHS) needs a strategy to prepare for unforeseen threats like these. And when the Federal government fails to effectively prepare, state and local officials must pick up the slack.

I’m very excited to hold today’s hearing here at Clemson University and grateful to the distinguished witnesses for testifying. We can’t predict when or where a ‘21st Century Hugo’ might hit us but I’m confident that the testimony from today’s panels can help us become more prepared for a variety of emergencies we may face.

###