



## Highlights:

[911 Outages Prompt FCC Inquiry](#)

[Revisiting Emergency Plans and Needs](#)

[Cyber Attacks "Death by a Thousand Cuts"](#)

[Outdoor Warning System Surveys Siren Policy](#)

## Disclaimer of Endorsement:

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.



The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit [www.usfa.dhs.gov/emr-isac](http://www.usfa.dhs.gov/emr-isac) or contact the EMR-ISAC office at: **(301) 447-1325** and/or [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov).

# The InfoGram

Volume 12 – Issue 42

October 25, 2012

## 911 Outages Prompt FCC Inquiry

The [Federal Communications Commission](#) (FCC) and Congress are investigating 911 system outages in Virginia and West Virginia caused by the storm system that passed through on June 30<sup>th</sup>. The outages lasted for hours or days in some regions and affected the 911 availability for more than a million people.

The outage is primarily being blamed on the loss of the commercial power grid due to wind and physical damage. Coupled with the failure and malfunction of the backup-power supplies used by private sector carrier networks, many are questioning some of the practices and policies used to govern the stability or availability of 911 systems.

The overall resiliency of 911 systems relies on many different pieces controlled by several different sectors. This should be a reminder for Public Safety Answering Points (PSAPs) nationwide to ensure they have a good working relationship with their carrier, that their network carriers have working backup power supplies in place, and those systems are tested or repaired often.

This incident has also served as a wake-up call to legislators, policy makers, and network carriers to make necessary regulatory adjustments to make sure outages like this don't happen again. The chief of the [FCC's public safety and homeland security bureau](#) stated "We should not – and do not – find it acceptable for 911 to be available reliably under normal circumstances.....but not available when a natural disaster occurs."

(Source: [Urgent Communications](#))

## Revisiting Emergency Plans and Needs

The 2011 east coast earthquake was a reminder that planning only for what is most expected is not enough. The quake was felt as far away as Georgia and Toronto, Canada. This year, tornadoes hit [Arizona](#) and [Queens, NY](#), hotshot teams from the west were sent to help with wildfires in [Virginia](#) and [Pennsylvania](#), and last week [Maine](#) had a 4.0 earthquake.

Exceptional events like those above give [affected regions a chance to reevaluate their response plans](#). It also gives the rest of the country an opportunity to apply

*The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.*

lessons from the event to their own region and plans, in this case planning for uncommon but high impact events.

Most authorities in the emergency management field suggest reviewing emergency plans at least yearly to make needed changes. The Federal Emergency Management Agency has several hazard mitigation guides which give step-by-step guidance on risk assessment procedures, including [Understanding Your Risks: Identifying Hazards and Estimating Losses](#).

(Source: [Homeland Security Newswire](#))

## Cyber Attacks “Death by a Thousand Cuts”

Ongoing cyber [denial of service](#) (DOS) attacks on United States financial institutions and businesses have [increased in recent weeks](#). Most companies reporting being hit are large corporations, possibly because they have the resources in place to identify a cyber attack while [smaller companies don't](#).

The Secretary of Defense described this as a “pre-9/11 moment” and gives specific examples of the [implications to infrastructure](#) to include the risk of a [foreign entity manipulating the electrical grid or water system](#). The head of the U.S. Cyber Command and director of the National Security Agency describes these attacks as “[death by a thousand cuts](#)” and refers to the loss of corporate trade secrets and technology as “the greatest transfer of wealth in history.”

These remarks directly reflect on national security as a whole, but the implications to the Emergency Services Sector should be strongly considered given its dependency on other sectors like water, energy, and communications. Partnerships with other regional stakeholders, joint exercises, planning, and cyber systems evaluations need to be worked out well before another serious national crisis.

(Source: [HSToday](#))

## Outdoor Warning System Surveys Siren Policy

2011 saw the highest number of tornado-related fatalities in 1 year since 1936. The [National Weather Service's 2011 assessment](#) (PDF, 4.32 Mb) cited outdoor siren policy and use as an “area of confusion” for communities.

The [University of Oklahoma and Indiana University of Pennsylvania are jointly conducting a survey](#) to help understand how outdoor weather siren technology is deployed across the United States and to determine the current policies and guidelines governing their use.

The expected outcome is to gather information from a wide range of siren networks around the country to better understand current realities of siren technology. The survey questions cover things like number and type of sirens, authority having jurisdiction, affected range in miles, and reasons the sirens are used.

People who oversee siren warning systems from all parts of the country are encouraged to complete the survey. The deadline is November 15, 2012. All information provided will be kept confidential and will not be used for any purpose other than academic research.

(Source: [Natural Hazards Disaster Research](#))

### Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes “fair use” of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond “fair use,” you must obtain permission from the copyright owner.

---

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local [FBI office](#) and also the [State or Major Urban Area Fusion Center](#).

---

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **[nicc@dhs.gov](mailto:nicc@dhs.gov)**.