



## Highlights:

Florida Firefighters Targeted in Drive-by Shooting

Recent Cyber Attacks Considered Game Changers

Guidance for Patient Decontamination

New Resource: Disasters. data.gov Launched

## 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 15 – Issue 1

January 2, 2015

## Florida Firefighters Targeted in Drive-by Shooting

A [drive-by shooting last week targeted firefighters](#) while they were outside the fire station pumping gas. There is little question they were targeted since they were in full uniform in a well-lighted area, right beside the fire station. One Jacksonville (FL) Fire and Rescue Department firefighter was hit by a ricochet bullet, but sustained minor injuries. A piece of apparatus was also hit by a ricochet. At this time, no one has been arrested.

In November, a [firefighter was shot and killed](#) during a standoff. The day before, [a man set fire to his house as a lure for first responders](#), ultimately shooting and killing a sheriff's deputy and wounding another. Though these two incidents were also in Florida, the rest of the country is obviously not immune to such violence and we have seen similar things happen in other states over the past few years.

Knowing also that there are growing reported threats towards law enforcement officers, all public safety and first responder personnel must take every precaution at active crime scenes, fires, medical emergencies, accidents, and any other possible event. An assailant may not take the time to notice what kind of uniform an officer is wearing, or they may not care.

(Source: [WJAX-TV](#))

## Recent Cyber Attacks Considered Game Changers

Several high-profile cyber attacks and breaches in 2014 brought considerable attention to cyber security and its consequences:

- The FBI arrested a woman after she allegedly [stole information from a secure federal database listing the vulnerabilities of United States dams](#), possibly for the Chinese;
- [North Korea's hack of Sony](#) is considered unprecedented, costing the company millions and perhaps requiring a year of analysis to [determine the true extent of the damage](#);
- Hacker group Lizard Squad is now [selling their Dedicated Denial of Service \(DDoS\) tool](#) online, allowing people to take down websites of their choice for as little as \$6/month.

The National Security Agency Director recently warned Congress that two or three countries are capable of shutting down the electrical grid and other critical systems

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

in the United States. He believes it [is a question of when, not if, such an attack will occur](#). Knowing that Congress still struggles with the legislative issues surrounding cybersecurity, it is increasingly up to the industries, companies, and agencies to protect themselves.

(Source: [FBI](#))

## Guidance for Patient Decontamination

The U.S. Department of Health and Human Services and Department of Homeland Security released new evidence-based guidance on decontamination, covering mass casualties, chemical release, external contamination, and decontamination of people. [Patient Decontamination in a Mass Chemical Exposure Incident: National Planning Guidance for Communities](#) is the country's first scientific-backed guidance.

Decontaminating patients who have come into contact with toxic chemicals can prevent or limit absorption, minimize impact, and decrease the chance of spreading the contaminant. Patient decontamination is considered a medical countermeasure as it protects health. Highlights from the guidance include:

- Determining need for decontamination of an individual patient and prioritization;
- Choosing patient decontamination methods;
- Determining the effectiveness of decontamination;
- Coordinating the system-wide response;
- Communicating crisis and risk messages to the community.

The guidance is based on the input of people and groups in the fields of emergency medicine, toxicology, risk communication, and emergency response, and also includes public comments.

(Source: [Public Health Emergency](#))

## New Resource: Disasters.data.gov Launched

Emergency managers have a new tool in their disaster response arsenal. Over the past 2 years since Hurricane Sandy so severely impacted the East Coast, ongoing meetings and discussions led to the development of [Disaster.data.gov](#) "to foster collaboration and the continual improvement of disaster-related open data."

The site contains information targeted towards different audiences, including emergency managers, first responders, and the public. The new website offers:

- A "Types of Disasters" Landing Pages: categorizes open data sets, apps, and tools to make relevant resources easier to find;
- Apps & Tools: includes apps and tools that can be deployed at minimal cost by first responders, emergency managers, volunteer organizations, and survivors;
- Innovator Challenge: highlights needs from the disaster preparedness community.

The website is also working to make select disaster-related datasets available. Often these datasets are closed to the public; working with the private sector and various levels of government to make the datasets public will provide communities with resources that can strengthen community resilience.

(Source: [Disasters.data.gov](#))

### 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).