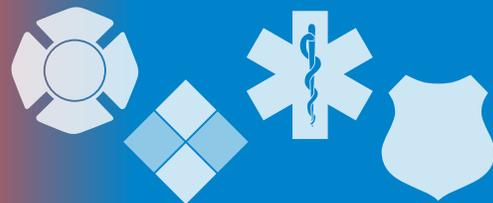


The InfoGram



Volume 19 — Issue 45 | December 12, 2019

Mass casualty incidents involving burns

The recent volcano eruption in New Zealand killed several people and left dozens of people hospitalized with severe burns. Many victims were still unaccounted for at the time of this writing but the threat of continued eruptions keeps recovery operations grounded.

Doctors treating the injured described the situation as horrific and said [hospital staff were sent out to get cling wrap to cover burns](#) as a temporary measure. New Zealand has [requested a significant amount of skin donations](#) from Australia and the United States to help with treatment. Patients are being transported to other hospitals to reduce the load to facilities and, in some cases, repatriate patients to their home country.

Burn mass casualty incidents (BMCI) usually exceed the resources of local hospitals to which victims are initially sent. Some incidents could even tax a dedicated burn center as they are often few and far between, covering a large geographical area. In 2016 the total number of beds at designated burn centers in the United States stood at approximately 1,800.

EMS providers, medical facilities, public health offices and other stakeholders should review the guide [Mass Burn Event Overview](#) (PDF, 319 KB) to bolster their BMCI plans and identify any gaps that may exist in policy and procedures. The guide covers initial burn care and stabilization as well as triage and transportation considerations.

Medical stakeholders need to work closely with emergency managers at all levels of government to ensure a tiered system of response is in place to provide burn patients optimal care. The guide discusses many aspects of this including triage patient tracking, supply support, mental health support and patient threshold numbers.

All stakeholders should be aware of the closest designated burn centers, its capacity and the procedures for working with them on a BMCI. There are maps and other resources available within this document.

This guide was produced by the U.S. Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response (ASPR).

(Source: [ASPR TRACIE](#))

Getting people to evacuate before a disaster

One of the banes of emergency management work is [convincing the public they need to evacuate](#) ahead of a forecasted emergency such as a hurricane or flood. Even after the hard lessons learned from Hurricane Katrina in 2005, only about half of the 350,000 included in New York City's mandatory evacuation order evacuated before Hurricane Sandy in 2012.

Officials use a variety of methods to convince people to leave their homes, including door-to-door canvassing and messages using a variety of media and



Highlights

Mass casualty incidents involving burns

Getting people to evacuate before a disaster

NG911 Self-Assessment Tool helps agencies assess readiness

Cyber Threats



U.S. Fire Administration

The U.S. Fire Administration operates 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 or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

[Subscribe here](#)



social media. Some tips:

- 🕒 Explain that first responders may not be able to reach them during the emergency.
- 🕒 Remind people that relief efforts may also be delayed by hours or days in the aftermath.
- 🕒 Describe the quantity of supplies they need until help arrives, 3 days' worth of food and water, prescription medicine, and other necessary supplies for each member of the household.

[Scare tactics](#) are controversial but some localities do use them. Requesting a resident's next of kin information or suggesting they let their family know [funeral assistance](#) is available through the Federal Emergency Management Agency (FEMA) in the event they die during the disaster might drive home the point, but the success of these tactics is unknown.

Make the idea of evacuation as easy as possible for people in your jurisdiction through effective communication. Provide as much information as is useful but don't overwhelm them. Give them one central location to find information. Also, be firm about dangers associated with emergencies in your region – but don't sensationalize them as that can lead people to tune out the message.

(Source: [Ready.gov](#))

NG911 Self-Assessment Tool helps agencies assess readiness

As a variety of different agencies work toward implementing Next Generation 911 (NG911) networks, assessing progress can be challenging.

Built on feedback received from government, industry and academia stakeholders, the [NG911 Self-Assessment Tool](#) is available to help administrators and oversight personnel evaluate a system's NG911 maturity state and understand the next steps necessary to continue deployment.

This easy-to-use checklist establishes common terminology and identifies key milestones to help 911 call centers understand the multi-year NG911 implementation process.

The tool is a downloadable Microsoft Excel file, which ensures that collected results are only shared with the agency completing the assessment. The Tool compiles respondents' answers and categorizes their 911 system into one of five maturity states for NG911 implementation.

Results are intended to help agency leadership: 1) document their 911 system's current functions and capabilities; 2) strengthen their understanding of NG911 elements; and 3) help outline next steps to transition their system into a fully integrated NG911 network.

Visit [911.gov](#) to learn more about the NG911 Self-Assessment Tool and other resources available for the NG911 transition.

(Source: [911.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.

Disclaimer of Endorsement:

The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Cyber Threats

Cherokee Nation cyberattack treated as domestic terrorism

Computer systems at the Eastern Band of Cherokee Indians were down after **a tribal employee allegedly attacked the network with ransomware** on Saturday, December 7.

Emergency services are still functioning and all departments will continue to operate as normal within the limitations imposed by the downed network, an official said. The tribe's financial information remains secure through the tribe's financial systems software provider.

(Source: [Smoky Mountain News](#))

Supply Chain Risk Management webinar for health sector

The Health Sector Cybersecurity Coordination Center (HC3) will host their monthly webinar threat briefing series to discuss **actionable cybersecurity threats and mitigation practices for the Healthcare and Public Health sector**.

The next briefing "Supply Chain Risk Management" is scheduled for December 19th, 2019, at 1 p.m. Eastern. Future briefings will be on a monthly basis. These unclassified briefings are open to professionals in the healthcare industry. To receive the webinar meeting details and more information, please contact HC3@hhs.gov.

(Source: [HC3](#))

Thieves using Bluetooth tech to find cars with gadgets inside

A recent rise in laptop and gadget thefts from cars, particularly in San Francisco and Bay Area, has left victims and police wondering if burglars are using Bluetooth scanners to choose target cars based on which have gadgets inside emitting wireless signals.

Criminal use of Bluetooth scanners has been dismissed by some as an urban myth. Maybe the burglar just watched the victim put their laptop bag in their trunk or hide it in the back seat. And given how common it is to leave valuable tech behind in a vehicle these days, it's not inconceivable that burglars are just playing the odds.

But **law enforcement officials have confirmed to WIRED that at least some burglars do use Bluetooth scanners to guide certain break-ins**.

(Source: [Wired](#))

Spice up your cybersecurity training with the escape room concept

Let's face it, no one likes cybersecurity training. The online courses are boring and, even though cybersecurity is critical, the time it takes to complete the training courses take away from the mission.

But what if - think about it for a moment - cybersecurity training was interactive, collaborative and - hold on - even fun?

That's what the Department of Health and Human Services attempted to do by hiring a vendor to **run a cybersecurity escape room** during Cybersecurity Awareness month.

(Source: [Federal News Network](#))

Cyber Information and Incident Assistance Links

[MS-ISAC](#)

SOC@cisecurity.org
1-866-787-4722

[IdentityTheft.gov](#)

[IC3](#)

[Cybercrime Support Network](#)

General Information Links

[FTC scam list](#)

[CISA alerts](#)

[Law Enforcement Cyber Center](#)

[TLP Information](#)

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