Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 19 — Issue 37 | October 10, 2019

2019 Tech to Protect Challenge needs your help

The 2019 Tech to Protect Challenge is coming to a city near you, and it needs first responders and emergency managers to serve as subject matter experts.

This is a federally funded contest in which coders develop more reliable tools and resources to meet specific challenges. First responders are encouraged to participate to provide context and help participants understand the challenges you face in your daily work.

There are 10 contests to develop technology focusing on things such as:

- Fire safety in 3D: incentivizing homeowners to create pre-incident plans for firefighters.
- Monitoring emergency responder health.
- Augmented reality to help save trapped passengers.
- Tracking patient triage.
- Placing deployable networks during emergencies.

There is still time to register for the event coming up from November 1-3, 2019. If you are in or near Los Angeles, Miami, New York City, Pittsburgh, San Francisco or Seattle, consider being a part of this interesting event.

As first responders and emergency managers, you face unique communications challenges. You can support a code-a-thon near you by serving as a knowledge resource for participants. Visit the Tech to Protect website to learn more about how you or your agency can get involved.

(Source: Tech to Protect)

CISA releases updated National Emergency Communications Plan

The Cybersecurity and Infrastructure Security Agency (CISA) released the updated National Emergency Communications Plan (NECP) last week. NECP is the Nation's roadmap to ensuring emergency communications interoperability at all levels of government.

CISA engaged more than 3,500 public safety representatives from federal, state, local, tribal and territorial public safety agencies, non-governmental organizations and other groups to ensure the NECP reflects the emergency communications expertise, experience and needs of the whole community.

The NECP addresses current gaps within emergency communications, reflects new and emerging technological advancements, and provides guidance to drive the nation towards a common end-state for communications. The updated NECP:

- Builds upon the key concepts and principles of the 2008 and 2014 versions of the NECP.
- Revises the vision statement to address secure information exchange and adds the public to acknowledge their increasing role in emergency communications.

Highlights

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

- Emphasizes the importance of strategic and lifecycle planning and sustainable funding.
- Promotes the importance of evaluating and documenting lessons learned from training and exercises.
- Underscores the need for coordination of communications assets and capabilities at incidents and planned events.
- Emphasizes technology and infrastructure lifecycle management and focuses on effective and interoperable information sharing.
- Adds a new goal focused on cybersecurity risk management, the mitigation of cybersecurity vulnerabilities, cyber hygiene minimums and funding.

(Source: CISA)

FirstNet apps catalog

As FirstNet development moves forward, one of the key components is a set of FirstNet-compatible apps for first responders to use. Similar to an app store, the FirstNet App Catalog is a one-stop shop for apps accepted into the program.

Security is an important feature. In 2017, the Department of Homeland Security found that more than half of mobile applications used by first responders had high-risk vulnerabilities. Providing secure tools was crucial to the FirstNet team.

Mobile apps listed in the FirstNet App Catalog are cleared through a certification program, reducing the risks of cyberattack or exploitation. Apps in the catalog fall into two categories: Certified and Reviewed. Both require a variety of checks, disclosures and evaluations; the Certified level also requires a source code scan.

Of the nearly 200 apps submitted for inclusion, about half made the cut, to include communications tools, crisis response platforms, mapping and GPS tools, and body cameras. FirstNet-related smartphones came on the market in August.

Those departments or agencies already working with FirstNet can contact their representative for more information on the FirstNet App Catalog. Those who are not yet working with FirstNet can request more information through its website.

(Source: FirstNet)

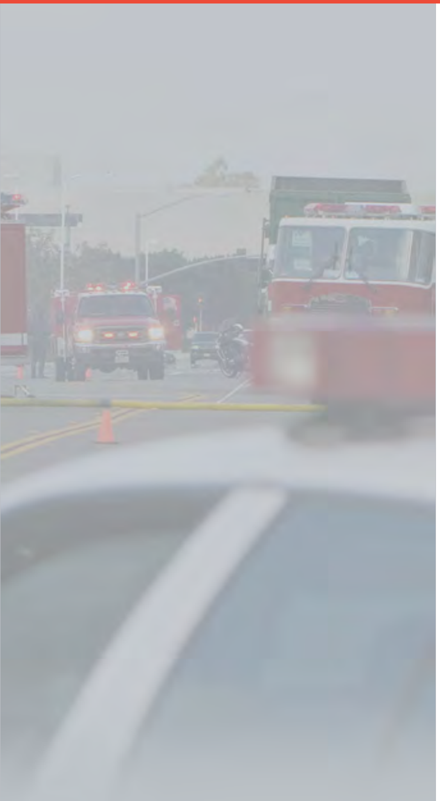
Great ShakeOut 2019: practice your earthquake drills

It's been another interesting year for earthquakes. 2019 has seen a 6.3 in Oregon, a 7.1 in California and several smaller ones reported in less seismically active states such as Tennessee and Pennsylvania. No matter where you live, it's a good idea to remind your community to practice earthquake drills.

Fortunately, the Great ShakeOut is next week, giving you a prime opportunity to spread the word about earthquake safety. The ShakeOut website offers social media materials, flyers, posters and other awareness resources you can use to encourage people to brush up on earthquake safety.

Over 18 million local governments, schools, tribes, businesses and more are participating in the ShakeOut on October 17. You can register your organization and see who else in your region is registered on the Great ShakeOut website.

(Source: Great ShakeOut)

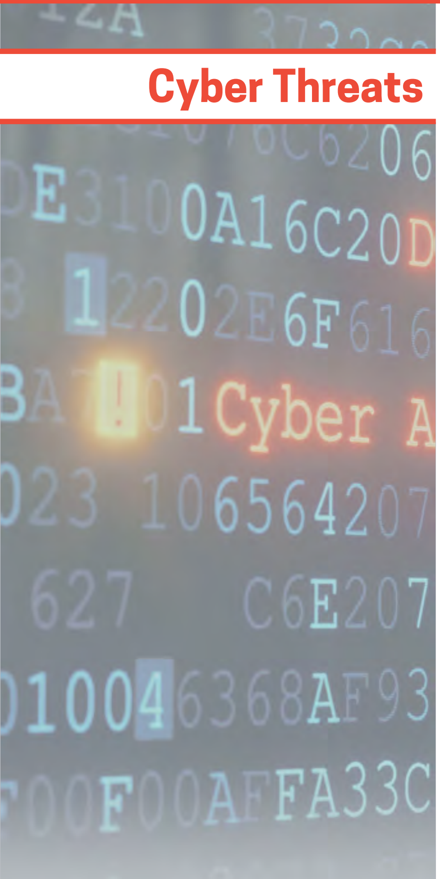


Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

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

FDA issues cybersecurity warning on medical devices

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." **These vulnerabilities may allow anyone to remotely take control of the medical device and change its function**, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

(Source: FDA)

Google Password Checkup searches web for leaked passwords

Google launched a new service called Password Checkup that will **check a user's saved passwords to see if they've been leaked or compromised in breaches**. Password Checkup is currently available for the Google web dashboard and Android devices, but will also be added to the Chrome browser later this year.

(Source: zdnet)

FBI says don't pay the ransom

The FBI Internet Crime Complaint Center (IC3) issued a public service announcement today regarding the increasing number of high-impact ransomware attacks against public and private United States organizations.

FBI urges all individuals or organizations that have been infected with ransomware not to pay the ransom but, instead, to contact their local FBI field office and report the incidents to ic3.gov as soon as possible.

(Source: Bleeping Computer)

Most malspam contains malicious URLs, not file attachments

In 2019, **85 percent of all malicious email spam (malspam) sent in Quarter 2 contained a link to a malicious file download**, rather than an actual malicious file attached to the email.

(Source: zdnet)

Ransomware attacks leave U.S. hospitals turning away patients

A rash of ransomware attacks this week targeted hospitals in the United States and Australia, freezing computer systems of several medical facilities to the point where they needed to turn away new patients and even cancel surgery.

Hospitals continue to be a top concern when it comes to ransomware attacks, given the sensitive nature of patient data collected by healthcare facilities.

(Source: ThreatPost)

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.