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

The InfoGram

Volume 19 — Issue 27 | August 1, 2019

Wildfire information and situational reports

With so much wildfire activity around the country, we thought it would be good to post a reminder of where to access current information and situational reports.

The National Interagency Fire Center (NIFC) in Boise, Idaho, currently lists the National Preparedness Level as 2 with 106 active large fires in 13 states. The NIFC publishes an Incident Management Situation Report (PDF, 915 KB), updated each morning at 7:30 Eastern. They also post the National Fire News – Current Wildfires, Monday through Friday.

InciWeb is another site providing information on active wildfires. It includes the name of the fire, cause, state and acres burned. The information is sortable. The site also includes maps of fire areas, pictures and video, announcements, road closures and links to their social media pages.

The U.S. Fire Administration (USFA) posts a Daily Operational Briefing for the fire and emergency services each morning Monday through Friday. It compiles reports on wildfire, hurricane, space weather and thunderstorm activity, and important national headlines that involve the emergency services. Subscribe to receive the Daily Operations Brief on the USFA Website.

In addition, you may check out individual state forestry websites where they have a variety of situation reports, maps, fire weather information and other updates.

(Sources: Various)

5G technology security may affect federal grants recipients

5G technology, the next generation of wireless networks, is becoming available in some areas of the country. While 5G provides faster service and other benefits to first responders, it also brings more security concerns. These concerns may affect first responders receiving grants or loans from the Department of Homeland Security (DHS) and other federal agencies.

Federal officials and the intelligence community are concerned about foreign involvement in the manufacture and development of 5G technology. Some companies manufacture semiconductors for smartphones or networking equipment, which could make it easier for foreign governments to hack devices and networks or collect user data. 5G will require new physical architecture, and much of this is manufactured by untrusted foreign companies.

Recent law prohibits federal agencies, federal contractors and recipients of federal grants and loans from purchasing equipment from some of the largest foreign telecommunications manufacturers. This may apply to recipients of DHS grants and loans.

Whether you receive grant money for communications devices or not, you can minimize potential security vulnerabilities by not purchasing equipment from the untrusted foreign manufacturers described in the 2019 National Defense Authorization Act (PDF, 9.5 MB).

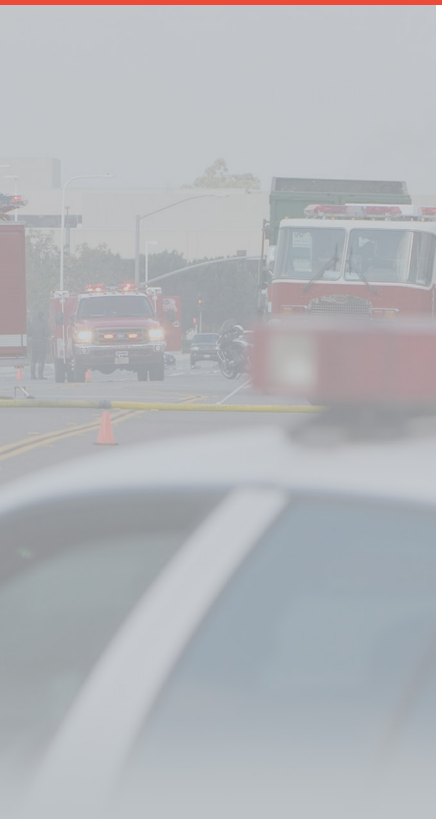
Highlights

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



The Cybersecurity and Infrastructure Security Agency (CISA) recently released the one-page "5G Wireless Networks: Market Penetration and Risk Factors" infographic and the "Overview of Risks Introduced by 5G Adoption in the United States" (PDF, 749 KB) bulletin detailing the concerns about the 5G supply chain, deployment and network security.

(Source: CISA)

Mass Casualty Trauma Triage Paradigms and Pitfalls

The new "Mass Casualty Trauma Triage Paradigms and Pitfalls" (PDF, 1.23 MB) from the Technical Resources, Assistance Center, and Information Exchange (TRACIE) provides a framework for prehospital EMS providers and hospital planners to consider when planning for mass casualty incidents (MCI).

The focus of the paper is to define key differences between typical MCIs and mass violence events, where the scene is unsafe and the situation fluid; the number of patients exceeds expected resources; and standard triage and treatment methods may fail.

The paper suggests the traditional triage approach used to train EMS providers in the United States for decades is no longer feasible to effectively respond to mass violence MCIs, such as active shooters or vehicle ramming. In addition to outdated methods, TRACIE says hospitals and prehospital providers are often lax about training for MCIs and have not sufficiently tested plans and procedures.

TRACIE makes several recommendations for stakeholders to consider. Among them are to include law enforcement in prehospital planning, providing them with some medical and triage training, and to ensure integration between prehospital and hospital response.

This paper also touches briefly on triage for other types of incidents including chemical, biological/epidemic/pandemic, burns, blasts, radiation, and pediatric issues.

(Source: TRACIE)

Webinar: Tribal-Federal-State Jurisdiction and Public Safety

The legalities and nuances of jurisdiction can be hazy when working with tribal governments. The upcoming webinar "Tribal-Federal-State Jurisdiction and Its Relationship to Public Safety in Indian Country" from the Justice Clearinghouse intends to clear up some of the confusion.

The webinar will take a look at the complexity of jurisdiction in Indian Country in historical context and features an analysis of the subsequent treaties and what they established in the recognition of tribal sovereignty. It will cover tribal challenges of providing police, court and probation services in their own communities.

It will also discuss the change from treaties to congressional acts, laws, court decisions and federal policies in order to understand the current state of jurisdiction. In addition to tribal representatives, this webinar is especially recommended for any agency regularly working with tribal public safety.

The webinar is scheduled for Tuesday, August 13, 2019, from 1-2 p.m. Eastern. Registration is required.

(Source: Justice Clearinghouse)

Cyber Threats

New Trojan blocks antivirus software

Security researchers have identified a Trojan dubbed Extenbro that serves adware and prevents infected machines from accessing software security updates and security-related websites. By using Domain Name Server (DNS) changing to block a machine's access to legitimate security websites, Extenbro effectively **disables anti-malware and anti-adware security software running on infected machines**.

(Source: BleepingComputer)

Security considerations in a BYOD culture

Privacy considerations and the potential that devices could be lost or stolen were some of the security concerns that emerged early on in the bring your own device (BYOD) movement. Gradually those concerns grew to include users accessing and transferring corporate data over unsecured networks. Then data leakage and malicious apps raised alarms.

From an attack landscape perspective, **these connected devices increasingly became (and remain) an attractive threat vector for attackers**. Innovation has rapidly changed the ways we use technology, which has delivered us to a place where the devices themselves are more sophisticated and have greater access to corporate information and other highly valuable assets, according to Bhargava.

(Source: DarkReading)

MS ISAC cleaning devices doc

Over the years, many of us have accumulated a mountain of CDs, hard drives, devices, online accounts and other mediums to store information that are outdated and unused. Outside of the key information you kept stored on purpose for long term use or retrieval, **it is good to periodically assess and dispose of unneeded storage media and information**. This month's newsletter from the Center for Internet Security (CIS) provides details on managing your information and data, as well as how to safely dispose of those pieces you do not need any longer.

At the bottom of the page, the CIS provides a free Word version of this information that your agency can brand with its emblem or logo and send to staff or personnel.

(Source: Center for Internet Security)

With hourly cyberattacks, is your local government safe?

According to a 2019 report from the International City Management Association, **approximately one in three local governments do not know how frequently their information system is subject to attacks,** incidents and breaches. Of those that do, 60 percent report they are subject to daily cyberattacks, often hourly or more.

Places such as Baltimore and Atlanta have been hit with massive cyberattacks in recent years, but it's not just major cities that are at risk of losing data or having their systems hacked. Smaller municipalities are also targets. Ultimately, hackers won't discriminate based on the type of government or system they target.

(Source: GovTech)

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.