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

The InfoGram

Volume 19 — Issue 21 | June 20, 2019

Hardening your supply chain for hurricane season

In a poll of 101 Fortune 1000 companies, 62 percent of companies impacted by the 2017 hurricane season said they were not completely prepared. The inability to deliver goods or services will ultimately affect hurricane response and recovery.

First responders and emergency managers in areas commonly hit by hurricanes should have an understanding how the private sector supply chain works, how it is affected by hurricanes and how to plan for these problems, because it is a question of when, not if, it will cause you problems.

Many but not all manufacturing and retail companies have logistics plans in place to ensure both the availability of product and fast response to hurricane-prone areas. It is a constantly evolving practice, though, as each season brings different challenges requiring new and better planning, especially as technology advances and new fixes to problems emerge.

This series of articles about supply chain disaster logistics and planning covers several topics of interest to the Emergency Services Sectors, such as pharmaceutical supplies, warehousing and stockpiling supplies, security, relocating assets and driver shortages.

Coordinating with private sector partners before any disaster is vital to creating lasting partnerships, minimizing misunderstandings and avoiding supply delays. This should include both large national companies and smaller local shops, as both have strengths in such a situation.

(Source: SupplyChainDive)

NIST updates guidance for authenticating responders

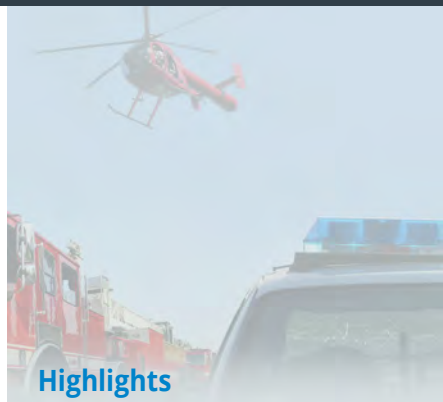
On-demand access to public safety data is critical to ensuring public safety and first responder (PSFR) personnel can deliver the proper care and support during emergencies. This involves heavy reliance on mobile platforms to access sensitive information. Complex authentication requirements can slow this down, and any delay—even seconds—can become a matter of life or death.

The National Institute of Standards and Technology (NIST) released the updated version of "Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders," its cybersecurity practice guide to secure applications used in emergencies for first responders.

This guide describes multifactor authentication and mobile single sign-on for native and web applications while improving interoperability. Those interested can download the complete guide or individual sections.

Organizations are encouraged to review the draft and provide feedback before the public comment period closes. Comments on this publication may be submitted by using the online comment form or by emailing psfr-nccoe@nist.gov. Public comments on the draft will close on June 28, 2019.

(Source: NIST)



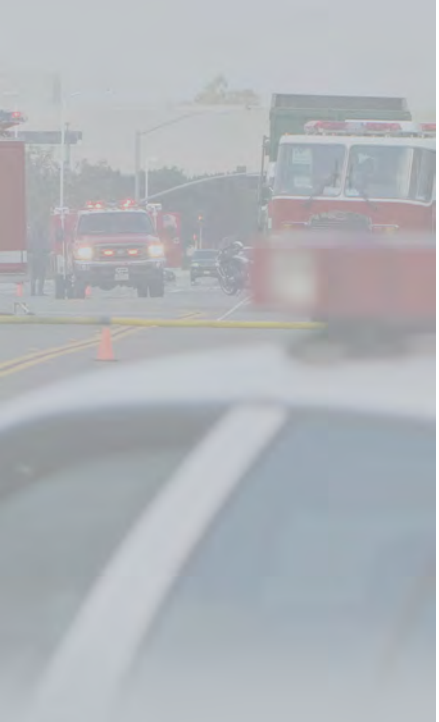
Highlights

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



New guide aids emergency planning for vulnerable populations

Vulnerable populations and at-risk communities account for a disproportionate number of fatalities seen in recent disasters. Many of those killed in California's Camp Fire last year were elderly and/or disabled and unable to evacuate. Wildfires in northern California's wine country in 2017 had a similar story: the Sonoma County Sheriff reported the average age of the deceased was 79.

Many emergency plans assume people have a certain ability to respond to and recover from emergencies. But some people have pre-existing vulnerabilities putting them in a precarious situation even before an emergency. For example, people on dialysis or needing insulin, or those with limited ability to see, speak, hear or understand. It is important to ensure people living with these kinds of conditions are addressed in emergency plans.

The National Association of County and City Health Officials (NACCHO) recently published a toolkit to address this issue. While the primary audience for "Capacity-Building Toolkit for Including Aging & Disability Networks in Emergency Planning" (PDF, 5.5 MB) is organizations within aging and disability networks, emergency managers and public health officials will find the wealth of information helpful.

The toolkit uses the terms access and function to define this population:

- Access refers to the accessibility of information, services and support critical to keeping the community healthy and safe.
- Function refers to restrictions or limitations an individual may have that requires assistance before, during and/or after an emergency.

In addition to readiness assessments, creating plans and general preparedness, the toolkit also discusses federal requirements, determining the size of the population needing support, communication and transportation considerations, and Americans with Disabilities Act compliance in sheltering.

(Source: NACCHO)

EARTH EX 2019 exercise and webinar

The EARTH EX Exercise is an international, multi-sector, virtual exercise focusing on processes and tools to support the response, restoration and community recovery from a long duration power outage caused by a Black Sky hazard. Black Sky hazards are events that catastrophically disrupt the functioning of critical infrastructures for a long period of time, such as a major cyber or physical attack, a strong electromagnetic pulse or a very serious natural disaster.

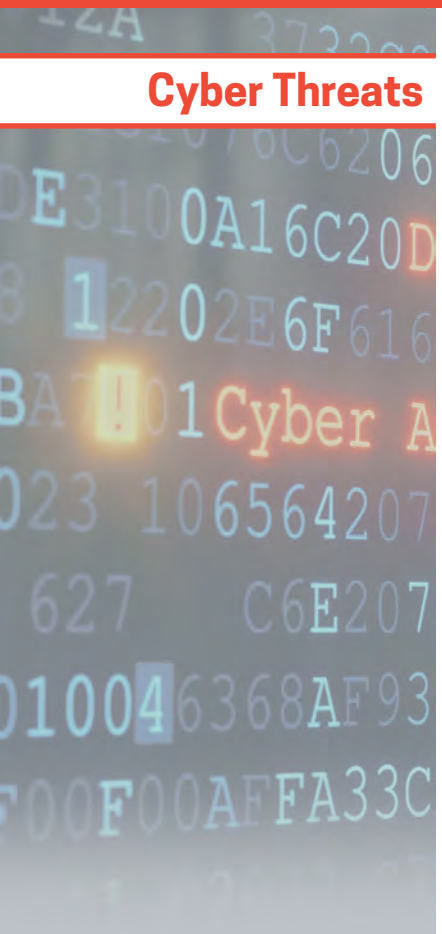
EARTH EX 2019, scheduled for August 21, utilizes National Information Sharing Consortium (NISC) tools to provide a full cross-sector wraparound experience. The focus this year builds on situational awareness techniques supporting decision making through multiple dynamic phases. EARTH EX 2016 is a one of a kind exercise opportunity.

On June 27, 2019, from 1-2 p.m. Eastern, the NISC will host a webinar with the Electric Infrastructure Security (EIS) Council on the EARTH EX 2019 Exercise to discuss how you and your organization can participate. This regionally focused event will provide participants with a unique opportunity to examine response and restoration postures.

Registration is required for this webinar. For more information, see the EIS Council website.

(Source: NISC)

Cyber Threats



New Phishing Scam Asks You to Manage Your Undelivered Email

A new phishing campaign is underway that pretends to be a list of undelivered email being held for you on your Outlook Web Mail service. This phishing email prompts you to decide whether you want to delete all of the emails, deny them, allow them to be delivered, or to whitelist them for the future. **Regardless of the link you click on, you will be brought to a fake "Outlook Web App" landing page that asks you to enter your login credentials**.

(Source: Bleepingcomputer)

2017 Equifax breach impacted online ID verification process

A recent report by the Government Accountability Office (GAO) highlights a relatively unknown dimension of the impact of the massive 2017 Equifax data breach. The standard method used by many government agencies for identifying United States citizens that want to apply for benefits through digital portals was rendered unsafe by the breach. And as it turns out, **some agencies are still using this unsafe method** today.

(Source: zdnet.com)

Security cameras most frequent IoT device targeted by hackers

Of all the Internet-connected devices that make up the Internet of things (IoT), **security cameras are most frequently targeted by hackers**, a new report by SAM Seamless Network shows. Security cameras account for 47 percent of devices on home networks that are vulnerable to cyberattacks.

Many of these attacks can bypass the security of cheap models of IP camera – with many of these low-cost devices based on a similar blueprint, meaning that if a vulnerability is found in one, it may also work against other models.

(Source: zdnet.com)

Congress wants to create cyber first responders

House lawmakers passed a bill June 10 that would require the **establishment of permanent "cyber incident teams"** to help protect both federal agencies and the private sector from cyberattacks.

The Department of Homeland Security (DHS) Cyber Incident Response Teams Act would create permanent teams of cybersecurity specialists within DHS that the government and industry could call on to help them recover from network breaches.

(Source: DefenseNews.com)

Five ways to increase your cybersecurity posture

Cybersecurity isn't easy, and there is no magic solution, but there are a handful of **things you can do that will greatly reduce your exposure to risk and significantly improve your security posture**. The goal is to increase the level of difficulty for an attacker to succeed in compromising your network and to improve your chances of quickly detecting and stopping attacks that occur.

(Source: TheHackerNews)

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.