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

The InfoGram

Volume 19 — Issue 44 | December 5, 2019

National Firefighter Registry to study cancer moves forward

Last year, Congress passed the Firefighter Cancer Registry Act requiring the Centers for Disease Control and Prevention (CDC) to create a registry to track and analyze cancer trends and risk factors in the United States fire service. The National Firefighter Registry (NFR) website is now live.

From the website: "All firefighters—structural and wildland, career and volunteer, active and retired—should consider participating in the NFR. This includes firefighters who have never received a cancer diagnosis, previously had cancer, or currently have cancer."

The NFR is a crucial initiative many people across the country fought for. Rates of some cancers appear to be higher in firefighters (PDF, 768 KB), but more study is needed to determine the true extent of the problem. This is especially true for volunteer, female and minority firefighters, as there is not as much collected data for these groups. Cancer researchers can use all the help we can give them to better understand the link between toxins, on-the-job exposure and cancer.

In the near future, all current and former firefighters will be able to help the fight against cancer by enrolling in the NFR. Fire service leaders should start discussing the registry with their staff now. Participation is completely voluntary but strongly encouraged. Leadership can boost participation by talking about the importance of this project with staff.

(Source: National Firefighter Registry)

Landslide Inventory Map web-based tool

The United States Geological Survey (USGS) developed a new web-based interactive landslide inventory map, available online free of charge. The USGS collected data from multiple federal, state and local government agencies to catalog landslide occurrences across the United States.

All states and territories experience landslides, though some areas experience them more frequently. Landslides can be incredibly destructive to property and life, though the latter is thankfully less common. Emergency managers should be aware of their regional landslide risks.

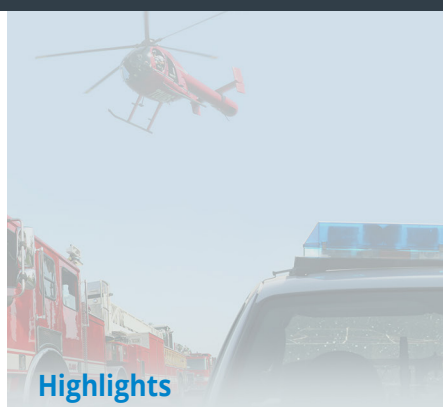
There are geographical areas not represented as more mapping is needed in those regions. The searchable map links to geospatial files where data are available. The database and map will be periodically updated.

(Source: USGS)

Washington Navy Yard shooting 6-year review

In September 2013, a contract employee entered a building at the Washington Navy Yard in the District of Columbia and wandered the halls shooting people for over an hour, ultimately killing 12 and injuring several more.

In the aftermath, local and federal agencies reviewed response gaps and adjusted plans and procedures accordingly. Often changes to plans or response procedures



Highlights

National Firefighter Registry to study cancer moves forward

Landslide Inventory Map web-based tool

Washington Navy Yard Shooting 6-year review

Webinar: HSIN Enhances the Public Safety of Tribal Governments

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

after a major incident can be handled as a one-and-done process. Revisiting lessons learned after some time has passed is a great way to make sure the necessary changes are really being made.

The District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA) recently held the Communications Interoperability Summit on "The Navy Yard Shooting Review: 6 Years Later" (PDF, 3 MB). The agencies involved in the 2013 shooting came together again to look over the incident response with a fresher eye.

Summit attendees also spent time re-examining after-action report recommendations, looking at how local and federal agencies addressed them, then updating the recommendations where necessary.

Most recommendations in this case involved communications; practices, procedures and policies; and experience and training. There are a number of practices mentioned that can help civilian jurisdictions and the military better respond to emergencies, no matter the type of incident:

- Establish better relationships between internal military emergency dispatching and their civilian 911 counterparts.
- Ensure civilian Computer Aided Dispatch systems include street names and addresses within secure or gated government or military locations.
- Security at military or government facilities should consider providing external responders with "go-bags" containing maps, floor plans, keys, important phone numbers and other such information. Security at office buildings or campuses should consider this also.

See the full 6-Year Review for more suggestions on creating better joint civilian-military emergency management and response. See also the after-action review conducted by the Department of the Navy (PDF, 2 MB).

(Source: Domestic Preparedness)

Webinar: HSIN Enhances the Public Safety of Tribal Governments

The Homeland Security Information Network (HSIN) can help tribal communities improve and safeguard their information for planning and operations. HSIN offers training, tools and support to improve their operations, secure their communications, access national resources and integrate with neighboring state and local agencies.

HSIN teamed up with the Cybersecurity and Infrastructure Security Agency's (CISA) Emergency Services Sector-Specific Agency (ES SSA) on the upcoming webinar "HSIN Enhances Public Safety Capabilities of Tribal Governments" scheduled for Wednesday, December 11, 2019, from 1- 2 p.m. Eastern.

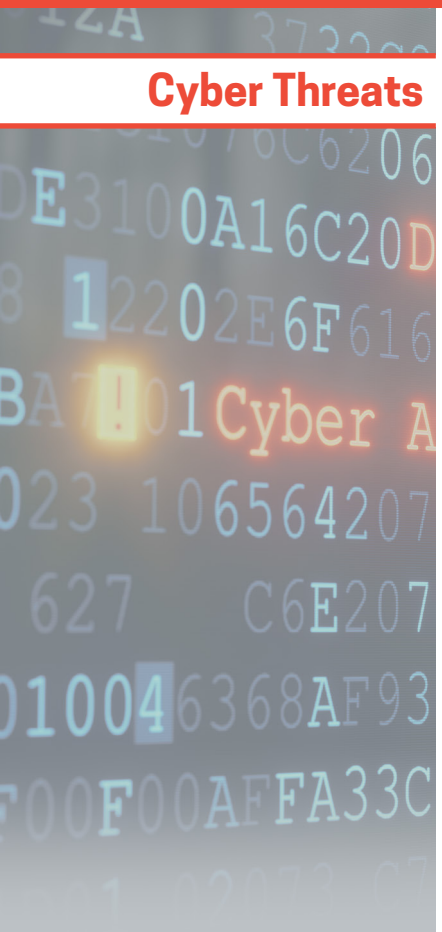
Presenters will share ways HSIN supports several tribal communities for special events, infrastructure security, public safety, law enforcement and intelligence operations with regional partners to keep their communities safe.

Registration is required for this webinar. The webinar link will be emailed to registrants; the call-in number is 800-895-8003.

Please forward this webinar information to anyone you think may be interested, especially tribal government personnel.

(Source: CISA)

Cyber Threats



Hackers want $25 million ransom for Texas ransomware attacks

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is planning to update the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181. The public is invited to provide input by January 13, 2020, for consideration in the update.

Comments received by the deadline will be incorporated to the extent practicable. The resulting draft revision to the NICE Framework, once completed, also will be provided to the public for further review and comment.

(Source: NIST)

FBI issues warning about smart TVs, hackers and personal security

Last week, the FBI's Portland field office warned Black Friday and Cyber Monday shoppers of the **potential risks that come with owning a Smart TV**. In addition to the inherent danger that your TV manufacturer and/or app developers could pose, there's the prospect that hackers could utilize some of the features on newer models to their advantage.

The existence of a microphone and camera in a Smart TV was solely meant to make life easier for the viewer, but placed in the wrong hands, these features can have an adverse effect.

(Source: Complex)

Cybersecurity getting more complex for state governments

State and big-city governments have stepped up their cybersecurity policies considerably over the past few years, officials said at a Department of Homeland Security conference outside Washington in September.

Several chief information security officers and homeland security advisers painted a rosy picture of state and local governments getting serious about enhanced training for public workers, more partnerships with other rungs of government and the private sector, and revising emergency response plans to cover cyberattacks. But they also acknowledged **they face an expanding threat landscape that endangers everything from government IT functions to critical public infrastructure**.

(Source: State Scoop)

How transparent should government be after a cyberattack?

In the past 18 months or so, cyberattacks on government have accelerated. Public-sector IT leaders have begun to view a successful cyberattack as a matter of when, not if.

Essentially, regardless of how well-prepared government is, a breach is still coming, and so **a larger onus is now being placed on response, specifically on best practices for the aftermath of a cyberattack**.

A question local government leaders must grapple with is this: How transparent should government be after a cyberattack? Should they tell citizens everything, or should they downplay incidents altogether, obscuring details under the assumption that any information on their vulnerabilities can and will be used against them?

(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.