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

The InfoGram

10 keys to improving public safety communications

Emergency alert, warning and notification (AWN) systems protect lives and property by identifying impending threat information, communicating information to those who need it and facilitating timely protective actions.

The Department of Homeland Security partnered with the National Council of Statewide Interoperability Coordinators and SAFECOM to publish "Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings and Notifications." The report lists ten best practices for emergency alert, warning, and notification (AWN) systems:

- Establish Governance.
- Identify and Coordinate with Others.
- Develop Plans, Policies and Procedures.
- Account for Diverse Populations.
- Maintain Security and Resiliency.
- Incorporate Safeguards.
- Train, Exercise and Test Systems.
- Eliminate Issuance and Dissemination Delays.
- Deliver Actionable Messaging.
- Monitor and Correct Misinformation.

Emergency managers and anyone else responsible for messaging during emergencies, including non-governmental entities, could benefit from a review of this report.

(Source: DHS)

FEMA releases updated Incident Command System (ICS) 300 and 400

The Federal Emergency Management Agency (FEMA) released updated 2019 versions of ICS 300 and 400 training (PDF, 242 KB) at the end of April. These courses are part of the National Incident Management System (NIMS) core curriculum.

- ICS 300, "Intermediate ICS for Expanding Incidents" provides training on and resources for overall incident management skills.
- ICS 400, "Advanced ICS for Complex Incidents" is designed for experienced responders and other senior personnel performing emergency management duties at complex incidents.

Because these courses contain new information based on the Third Edition of NIMS (October 2017), you may find it informative to review the new, updated versions. However, if you have successfully completed a previous version of these courses,

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

there is no FEMA requirement to retake the revised version of the course.

More information on the NIMS curriculum is available through the Emergency Management Institute.

(Source: FEMA)

Recent drone activity roundup

A number of newsworthy items have surfaced recently pertaining to unmanned aerial systems (UAS, or “drones”).

In December, UAS activity near several major airports in the United Kingdom disrupted travel plans for 140,000 airline passengers. 2018 was an active year overall for UAS in the country. The operator in the December incident still has not been caught. The potential for a catastrophic incident with a high loss of life is a serious concern for transportation authorities and emergency services alike.

Recently a man was charged with violating secure airspace after operating a drone to dump political leaflets over two major football games in California. This is especially concerning for those responsible for security of public venues, as the potential of drone use for criminal or terrorist activity is limited only by the actor’s imagination.

UAS capabilities in disasters is also getting some interest, such as from this architect interested in designing hospitals able to accept drone delivery of food, medicine or other supplies when roads and infrastructure are destroyed.

And for those departments interested in UAS use in emergency work, this New Hampshire sheriff’s office is training drone operators and police dogs to work together when searching for missing people and criminals. The high-tech drones have thermal imaging cameras and speakers, so officials can call out to people. Teams are learning to coordinate the low- and high-tech resources.

UAS capabilities and innovation – whether commercial, artistic or destructive – continue to evolve, and it will take just as much innovation to keep up with those using them for nefarious purposes.

(Sources: Various)

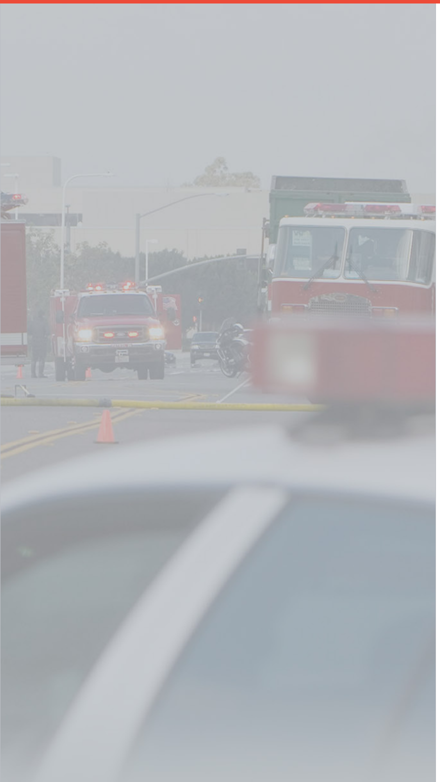
First Responder’s Toolbox: full catalog of documents

For ease of use, the Joint Counterterrorism Assessment Team (JCAT) has updated and provided a comprehensive catalog of all the First Responder’s Toolboxes published between December 2013 and April 2019 (PDF, 2 MB).

The graphic side of this document is broken down by target and highlights the various Toolboxes which may assist customers in counterterrorism outreach, education and training.

The non-graphic side of the catalogue includes a list of **all** First Responder’s Toolboxes to include terrorist techniques, tactics, and procedures, and terrorism prevention topics. Please also note the customer friendly key following each Toolbox title which highlights how to access the product, what format the product is in and if the product is available in Spanish.

(Source: JCAT)



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

Free web scanning resources

The Department of Health and Human Services (HHS) recently published a list of free web scanning resources to help organizations identify and manage web vulnerabilities (PDF, 1.2 MB). **Web vulnerability identification and management is a never-ending process**, as new vulnerabilities are identified all the time.

This briefing defines the problems associated with web security and vulnerabilities and lists numerous free scanning tools organizations and agencies can use to look for website errors, trojans and malware.

HHS recommends the Cyber Hygiene: Vulnerability Scanning tool offered by the Department of Homeland Security to assist in securing internet-facing systems.

(Source: HHS)

Cyber espionage against public sector increasing

International spies are hitting government networks harder than ever, according to the latest Verizon Data Breach Investigations Report released Wednesday. The 2019 report shows a 168 percent increase year-over-year in the number of government network breaches linked directly to state-sponsored actors. **The growth solidifies cyber espionage atop the list of threats to the public sector for the second year in a row**.

(Source: NextGov.com)

RobinHood ransomware targeting government networks

Baltimore city government is still offline following a RobinHood attack. Officials confirmed the RobinHood virus infected city servers sometime early last week.

According to information from the National Capital Regional Threat Intelligence Consortium, a new type of ransomware, dubbed RobinHood, is actively targeting government networks in the United States. First discovered in April 2019, RobinHood targets entire networks and attempts to encrypt files on as many computers on the networks as possible. The distribution method used to infect systems is currently unknown; however, the threat actors behind the campaign may be compromising remote desktop services or using Trojans to deliver the ransomware.

(Source: WBAL)

Webinar: National Critical Functions

The Cybersecurity and Infrastructure Security Agency (CISA) recently released a list of 55 National Critical Functions – functions of government and the private sector so vital to the United States that their disruption, corruption or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Join next week's webinar on Monday, May 20, 2019, from 1-2 p.m. Eastern to learn more about how National Critical Functions provide an evolved construct for critical infrastructure risk management; how the set of functions will provide the basis for deeper analysis to build a Risk Register; and how public and private sector partners can collaborate with CISA throughout this process. Registration required.

(Source: CISA)

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.