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

The InfoGram

Volume 19 — Issue 20 | June 13, 2019

Increased vigilance for Independence Day festivities

While enjoying the commemorative events and festivities surrounding Independence Day, please be sure to watch for any suspicious activity and report it. There are no specific, credible threats at this time, but foreign and domestic extremists see mass gatherings as prime targets, especially national or religious holidays.

In 2018, the FBI arrested a man who was planning to detonate a bomb in downtown Cleveland during Fourth of July celebrations. He was allegedly plotting to help al-Qaida.

Certain activities can be indicators of a future or imminent threat and should be reported. Examples of suspicious activity:

- Stolen explosives, fireworks, chemicals, uniforms, access cards or keys.
- Unattended packages, bags, or boxes.
- Extended or repeated surveillance of an area or building.
- Someone asking questions about security, shift changes or operations.
- False or diversionary emergency calls.
- Someone dressed in clothing not appropriate to the weather.

The Department of Homeland Security's See Something, Say Something campaign provides information to first responders and the public on what to look for and who to report it to. They even have a series of videos to test your attention to detail.

There is plenty of time to have employees take the Nationwide SAR Initiative's (NSI) free online Suspicious Activity Reporting (SAR) training, targeting audiences such as Fire/EMS, emergency management, PSAP/9-1-1 dispatchers, private security and public health/healthcare. They also provide resources on SAR reporting.

(Source: Nationwide SAR Initiative)

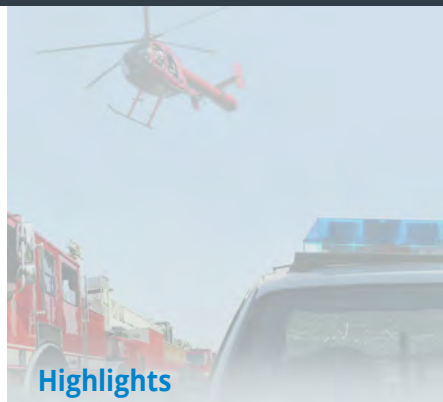
Webinar: Hostile Event Preparedness for the Community of Faith

On Thursday, June 20, 2019, at 1 p.m. Eastern, the Faith-Based Information Sharing and Analysis Organization (FB-ISAO) is hosting the webinar "Hostile Event Preparedness for the Community of Faith."

This webinar will cover active shooter incidents, workplace violence and workplace attacks, lone actor and low-tech terrorism, complex coordinated terrorist attacks, fire as a weapon, weapons of mass destruction, and other related activities.

It is vital to understand the ever-changing threat environment and to base preparedness activities on a threat-informed and risk-based approach. This webinar presents threat analysis, actionable recommendations, and best practices.

First responders have a prime opportunity to invite leaders from local houses of worship to take part in this webinar as a team, promoting communication and security best practices. Partnerships, joint planning meetings and exercise sessions



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

between the faith-based community and first responders can only benefit all involved.

Registration is required to attend and there are a limited number of spaces. We highly recommend getting everyone interested together under one registration to allow as many participants nationwide as possible. If the webinar fills up, more sessions may be scheduled.

Visit the Federal Emergency Management Agency (FEMA) website for more information on protecting houses of worship.

(Source: FB-ISAO)

What's New in Blue video series

The Department of Justice's Community Oriented Policing Services (COPS) began a new video series "What's New in Blue" to keep law enforcement up-to-date on critical issues and innovative developments in law enforcement. They are similar to the popular TED Talks: short, one-topic talks ideal for adding to a training program or sharing with colleagues.

Six episodes are available so far in Season 1, including topics like "Dispatch Response During Active Shooter Events," "Policing in Indian Country," Interdiction for the Protection of Children," and "Coordinated Response to Mass Casualty Events." As you can see, topics vary widely and can be beneficial to other fields in addition to law enforcement.

Videos are available on the COPS website and COPS Office YouTube channel.

(Source: COPS)

New FEMA guide New Recipients of Disaster Grants Guide

FEMA recently published the "New Recipients of Disaster Grants Guide," a centralized resource document providing state, local, tribal and territorial governments guidance on the essentials of Public Assistance (PA), Individual Assistance (IA), and Hazard Mitigation Grant Program (HMGP).

The guide combines pre-disaster preparation recommendations, program requirements, associated deadlines and other information from all three grant programs. The guide also outlines the critical statutory, policy and procedural requirements for recipients of FEMA disaster assistance grants.

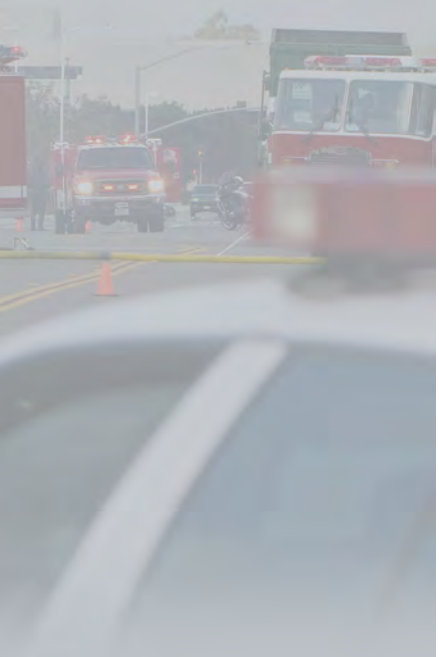
The scope of the guide includes pre-disaster preparations and post-disaster actions and is tailored to an audience of current (or prospective) recipients of federal disaster grant funding.

Join one of FEMA's two upcoming webinars to learn more about the New Recipients of Disaster Grants Guide:

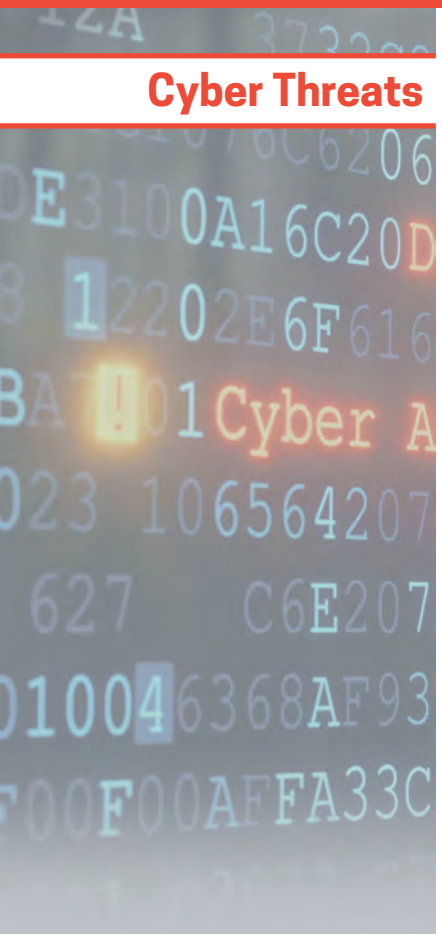
- Webinar 1: 2 p.m. Eastern on Monday, June 17, 2019.
- Webinar 2: 2 p.m. Eastern on Wednesday, June 19, 2019.

The FEMA Teleconference call-in number is 1-800-320-4330, PIN 859916#. If you need a copy of the webinar PowerPoint, please provide details on the registration page or contact jacob.rodrigueznoble@fema.dhs.gov.

(Source: FEMA)



Cyber Threats



How to remove yourself from the internet

If you're reading this, it's highly likely your personal information is available to the public. And "public" means everyone everywhere. So, how can deleting yourself from the internet prevent companies or people from acquiring your info?

Short answer: it can't. Unfortunately, **you can never remove yourself completely from the internet, but there are ways to minimize your online footprint**, which would lower the chances of your data getting out there. Here are some ways to do just that.

(Source: Cnet)

Interns seen as a goldmine for hackers

Many departments and agencies are in the process of hiring interns for summer work. While these programs are often beneficial to everyone involved, keep in mind **an intern's lack of understanding (or proper training) on information security coupled with their use of social media can hand a hacker a wealth of information** that can then be used against your organization.

(Source: SecurityIntelligence.com)

Intelligence update: ransomware threat to state, local government

The Health Sector Cybersecurity Coordination Center (HC3) released the following TLP: white threat intelligence briefing report "Ransomware Threat to State & Local Governments" (PDF, 1.8 MB). **This report covers the ransomware threat to all sectors**, not just for the Healthcare Public Health Sector.

(Source: HC3)

Should failing phishing tests be a fireable offense?

Would your average Internet user be any more vigilant against phishing scams if he or she faced the real possibility of losing their job after falling for one too many of these emails? Recently, I met someone at a conference who said his employer had in fact terminated employees for such repeated infractions. As this was the first time I'd ever heard of an organization actually doing this, I asked some phishing experts what they thought (spoiler alert: they're not fans of this particular teaching approach)...

(Source: KrebsonSecurity)

Hurricane season brings cyber threats targeting disaster victims

As the 2019 hurricane season begins, the Cybersecurity and Infrastructure Security Agency (CISA) warns users to **remain vigilant for malicious cyber activity targeting disaster victims and potential donors**.

Fraudulent emails commonly appear after major natural disasters and often contain links or attachments that direct users to malicious websites. Users should exercise caution in handling any email with a hurricane-related subject line, attachments, or hyperlinks.

If you believe you have been a victim of cybercrime, file a complaint with the Federal Bureau of Investigation Internet Crime Complaint Center at www.ic3.gov.

(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.