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

The InfoGram

Volume 20 — Issue 13 | March 26, 2020

COVID-19 cost recovery for fire and EMS departments

Fire and EMS departments responding to the COVID-19 pandemic may be able to recover associated costs through the Federal Emergency Management Agency's (FEMA) Public Assistance Grant Program. COVID-19 response has the potential to significantly impact departmental budgets.

If you think your department may apply for assistance, it is vitally important to keep records of expenses and usage costs as submission requests must completely and accurately document these costs. These may include but are not limited to:

- Overtime or personnel backfill costs.
- Expendable supplies including disinfectants, PPE and medical supplies.
- Apparatus usage.

Further federal guidance to support communities in this pandemic to include financial means is not yet finalized.

For more detailed information, see the U.S. Fire Administration's website. Please also see the "Procurement Under Grants Conducted Under Exigent or Emergency Circumstances" (PDF, 396 KB) and the FEMA website.

(Source: USFA)

Mutual Aid Resource Planner

In the aftermath of a disaster, emergency responders regularly rely on mutual aid support from neighboring towns to help response and to cover the area while recovery efforts continue, which can take days or longer. It is important to have such plans already in place; scrambling for regional assistance at the last minute takes time out from important life-saving measures.

In its research on improving mutual aid partnerships, the Department of Homeland Security's Science and Technology Directorate developed an application to help jurisdictions create better mutual aid plans.

The Mutual Aid Resource Planner (MARP) allows planners to develop capability-based mutual aid plans using a cloud-based platform, enabling rapid deployment and streamlining information sharing. The MARP:

- Allows users to share plans and resource needs with partners;
- Helps align planners with operations staff;
- Provides a simplified planning template.

This application has gone through testing and is now operational and available. Access to MARP requires a membership to the National Information Sharing Consortium (NISC). NISC membership is at the organizational level, and multiple people can be covered under the membership.

(Source: DHS S&T)

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

Improving your risk and crisis communication

Every emergency or disaster tests an agency's response, plans and operations. While now is not the time to take on a review and refresh of your plans, it's a good idea to consider it for the future. Over the next few weeks we will offer some guidance for agencies to utilize in future reviews and after action reports on a variety of topics.

"Communicating in a Crisis: Risk Communication Guidelines for Public Officials" from the Substance Abuse and Mental Health Services Administration (SAMHSA) reminds us the primary rule for risk communication is first do no harm. Crises frighten people and create the opportunity for misunderstanding and overreaction. It's important to plan what to say carefully. The guide offers these other tips:

- Decide what information is likely to prompt appropriate public actions.
- Identify obstacles to effective messaging and how they can be avoided.
- Anticipate the kinds of questions the public will have.

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) guide "Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators" (PDF, 908 KB) gives research-driven recommendations for creating and disseminating effective messaging. It covers audience involvement, establishing and keeping trust, and reaching out to special populations. Other things discussed:

- Communicating the need to accept risk and the costs incurred.
- Preparing to continue support even after the crisis is over.
- Restoring and repairing the organization's image.

The 2019 article "The Value of Crisis Communications" from Domestic Preparedness talks about the role of the Public Information Officer (PIO) as a vital component to response efforts. Also from this article:

- How the 21st century has redefined media.
- What to convey in the initial messaging.
- Using the media as a force multiplier to get accurate information to the public.

Consider bookmarking these resources for future plans reviews.

(Source: Various)

Webinars: Coping with COVID-19: Best Practices for Police, Fire/EMS

FirstNet is hosting two webinars on managing COVID-19 response. **Note that both webinars are being recorded**.

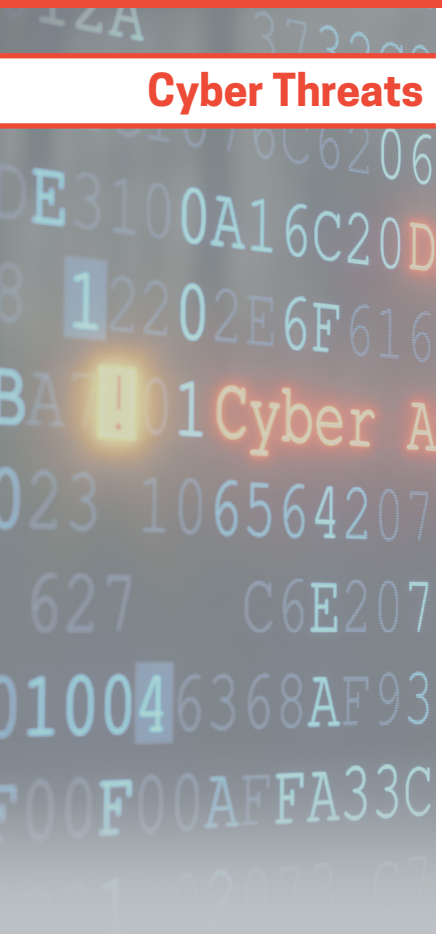
"Coping with COVID-19: Best Practices for Law Enforcement," set for Friday, March 27, 2020, from 1:30-3 p.m. Eastern.

"Coping with COVID-19: Best Practices for Fire/EMS" was held Thursday afternoon. Look for a link to the recording soon on the FirstNet website.

Learn directly from officers at major metropolitan departments how first responders on the front lines are handling patient engagement and operations; dealing with potential infections among their own; preparing and sanitizing stations and equipment; and ensuring they have the technology they need to effectively communicate.

(Source: FirstNet)

Cyber Threats



South Carolina fire district electronic systems hacked

On March 15, the Bluffton Township Fire District's electronic systems were hacked.

Officials said in a press release that during the day personnel reported district-wide issues accessing server information, reporting systems and everyday computer programs. Staff reviewed the issued and discovered the systems had been encrypted by an outside source. According to officials, a message was accessible to contact the perpetrators for information on releasing the computer data.

(Source: Fox 28)

Hackers use HHS.gov "open redirect" to push malware

An HHS.gov open redirect is being used by hackers to push malware payloads onto unsuspecting victims' systems with the help of coronavirus-themed phishing emails.

Open redirects are web addresses that automatically redirect users between a source website and a target site, and are regularly used by malicious actors to send their targets to phishing landing pages or to deliver malware payloads under the guise of legitimate services.

HHS.gov is the website of the Department of Health and Human Services which makes this specific open redirect the perfect tool to lure in potential victims.

(Source: Bleeping Computer)

What should you do instead of paying the ransom?

Thirty percent of federal agencies have experienced a ransomware attack within the last three years, according to the 2019 study, "Ransomware Threats: Is your Agency Ready?" In one of the most disastrous attacks, a variant called RobinHood hit Baltimore in May 2019. Obeying the instructions of the FBI and law enforcement, the city refused to pay the ransom of $76,000 and ended up spending $10 million on data recovery and losing $8 million because services like bill payments and real estate transactions were shut down for two weeks.

What should agencies do? Pay up and hope for the best, or refuse and risk prolonged downtime and an expensive recovery? Fortunately, there's a better option: Agencies can take action now that will help them avoid ever having to make this unpleasant choice.

(Source: GCN)

Remote work must be both reliable and safe

The global COVID-19 pandemic is forcing more employees to work from home everyday, and with each of us connecting to our household's router to carry out record numbers of Zoom calls, the pressure on broadband networks to support unprecedented demand for connectivity is building up.

As the pandemic affects more industries and threatens jobs in all fields, however, there has been increasing focus on ensuring that connectivity is not only reliable, but that it is also accessible for all that need it – a challenge that is likely to only grow in the near future.

(Source: zdnet)

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.