# The InfoGram

## Updated COVID-19 resources for first responders and local government

COVID-19 information is getting updated so fast it's easy to want to tune out; unfortunately, those working in emergency management and response can't afford to do that. Here is a brief rundown of links to current guidance and surveillance sites:

- Centers for Disease Control and Prevention (CDC) has a situation summary and list of updated cases in the United States. It also has guidance for first responders, healthcare providers, health departments, institutes of higher education and more.

- The U.S. Fire Administration now has a page dedicated to COVID-19 information with resources to help your fire, EMS and PSAP department prioritize infection control and screen patients either over the phone or in person. The page also links to further resources.

- Johns Hopkins University Coronavirus Resource Center interactive worldwide map is updated regularly with total cases, total recovered and total deaths by country.

- The CDC also just published "Implementation of Mitigation Strategies for Communities with Local COVID-19 Transmission" (PDF, 223 KB), a 10-page guide for state and local health departments.

- The Environmental Protection Agency lists disinfectants for use against COVID-19.

- The Occupational Safety and Health Administration provides employers and workers with information about staying safe on the job.

- The World Health Organization has online training for a variety of audiences.

(Source: Various)

## Firefighter Survival Safety Stand Down Week: June 14-20, 2020

The theme for this year's Firefighter Safety Stand Down is "Building a Superhighway to Safety – Protecting our Responders on Roadways." Departments and personnel are strongly encouraged to focus on safety and health education during this week, especially related to this year's theme of roadway incident safety.

It's been an especially bad year already for roadway-related injuries and fatalities. This week can give your department an opportunity to review techniques, operating procedures and learn new skills related to roadway operations.

An entire week is provided to ensure all shifts, volunteer members and all personnel can participate. Topic information, training downloads and videos will be available at the official website for the Firefighter Safety Stand Down.

Safety Stand Down is a joint initiative of the International Association of Fire Chiefs, National Volunteer Fire Council and the Responder Safety Institute.

(Source: Safety Stand Down)

### Highlights

Updated COVID-19 resources for first responders and local government

Firefighter Survival Safety Stand Down Week: June 14-20, 2020

Public Safety & Law Enforcement Toolkit for Unmanned Aerial Systems

Lessons learned at healthcare facilities during the 2017, 2019 wildfires

**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**

## Public Safety & Law Enforcement Toolkit for Unmanned Aerial Systems

The Federal Aviation Administration (FAA) has added more resources to its online UAS toolkit to assist law enforcement and public safety departments better handle incidents involving Unmanned Aerial Systems (UAS), also known as drones.

The most recent addition is the Public Safety Small Drone Playbook (PDF, 6.3 MB), a reference for officials conducting investigations involving UAS. This reference can assist you in determining the difference between authorized and non-authorized drone operations and guide you on what actions you might be able to take. It also:

❯ Provides a one-page quick reference guide on prohibited drone operations.

❯ Defines your authority under federal laws and what might apply under local regulations.

❯ Lists who to call for more information or assistance with UAS-related incidents.

❯ Shows examples of FAA-provided UAS certificates, registration, and waivers that UAS operators might show you.

❯ Gives suggested questions you might ask the UAS operator.

The rest of the FAA's toolkit includes the video "Know Your Authority," printable pocket cards, guidance document for suspected unauthorized UAS operations and other information.

(Source: FAA)

## Lessons learned at healthcare facilities during the 2017, 2019 wildfires

The latest issue of The Exchange (PDF, 6 MB) newsletter from the Technical Resources, Assistance Center, and Information Exchange (TRACIE) shares lessons learned by medical facilities and communities in recent Colorado and California wildfires.

The issue offers real-life experiences from 2017 and 2019 wildfire response focusing on evacuation, patient tracking, managing planned power shutoffs and planning for the future.

Three of the seven articles in the issue deal with challenges medical facilities face when dealing with planned power outages. Outages increase risk to everyone involved and there should be a strategy to prioritize power usage to manage the shortage.

Facilities also need to expect an influx of people who use electricity-dependent medical equipment at home (e.g., ventilators or oxygen machines) as these individuals may be forced to seek out care at a medical facility with backup power.

One tool available to help public health officials and medical facilities plan for this is the emPOWER Initiative. emPOWER is a secure, restricted mapping tool to help state and local health departments plan for and manage the needs of electricity-dependent Medicare beneficiaries in a geographical area. The resource is a great tool to help you meet the needs of one of your at-risk populations.

This issue of The Exchange also covers mass sheltering, hospital evacuation, managing stress and compassion fatigue among workers, and community recovery. It holds a number of important lessons and should be reviewed by hospital emergency managers and administration for planning purposes.

(Source: TRACIE)

## Cyber Threats

# State officials warn of potential coronavirus financial scams

The Pennsylvania Department of Banking and Securities is urging Pennsylvanians to be wary of potential financial scams trying to take advantage of the coronavirus situation. Officials said the following are tactics employed by scammers that residents should watch out for:

- **Sense of urgency and limited time offers**. No government agency will call you asking for payment or take punitive action against you if you don't act quickly.

- **Payment with wire transfer or gift cards**. Once information is provided, the money is essentially gone and you cannot get it back.

- **Secrecy and the need to not tell anyone**. Never make a decision without consulting a credible and trustworthy source.

- **Low or minimal risks with guaranteed high returns**. Be cautious of any offer that guarantees a high rate of return with little or no risk.

- **Unsolicited offers, including social media avenues**. A new post on your Facebook wall, a tweet mentioning you, a direct message, an email, a text, a phone call, or any other unsolicited communication regarding an investment "opportunity" related to coronavirus (COVID-19).

(Source: MSN)

# Ransomware increasingly targeting small governments

Small and local government have not only continued to pay ransoms to the criminals behind ransomware, but they have been doing so at an accelerating pace, according to a new report by a consulting firm. "**The more they are paying out, the more money criminals are demanding**," a researcher said.

Three unique facets of local governments are likely driving the increase in ransomware cases: The organizations tend to have insurance, they leave gaps in their networks and system security, and they need to maintain critical services. The result is a feedback loop.

(Source: DarkReading)

# Ryuk ransomware behind Durham, North Carolina cyberattack

The City of Durham, North Carolina has shut down its network after suffering a Ryuk Ransomware attack this weekend.

To prevent the attack from spreading throughout their network, Durham has "temporarily disabled all access into the DCI Network for the Durham Police Department, the Durham Sheriff's Office and their communications center".

This has **caused the city's 911 call center to shut down and for the Durham Fire Department to lose phone service**. 911 calls, though, are being answered.

While they have not seen signs that data has been stolen, the city has warned that users should be on the lookout for phishing emails pretending to be from the City of Durham.

(Source: BleepingComputer)

## 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.