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

# The InfoGram

Volume 20 — Issue 5 | January 30, 2020

## FirstNet deployables: what you should know before making a request

FirstNet offers a fleet of deployable assets, such as Satellite Cell on Light Trucks (SatCOLTs) and aerial cell on wings, to assist public safety communications during disasters and planned events. FirstNet's deployable asset program has shown so much success that the program expanded the fleet in 2019. These services are at no extra charge for subscribers.

In its recent newsletter to emergency managers, FirstNet outlined things emergency managers can do to effectively use these deployables. This information was originally presented at the All-Hazards Incident Management Team Association (AHIMTA) Training & Education Symposium.

Before making a request, you should understand your communications needs, the incident conditions, and terrain and access limitations. Coordinate with other jurisdictions who may have also requested FirstNet deployables. For planned events, 30-day notice is required.

It also recommends pre-planning for FirstNet services. If you are in a hurricane-prone zone, for example, you can identify potential set-up locations well in advance. Also, it recommends not assuming an event request was made, always submit a form.

Sign up for FirstNet's topical newsletters to follow developments for fire, law enforcement, EMS, emergency management and 9-1-1.

(Source: FirstNet)

## Justice Department changes drone rules in policy update

The Department of Justice (DOJ) released its updated Policy on the Use of Unmanned Aircraft Systems (UAS) in November 2019. The updated policy promotes the use of UAS technology only in connection with properly authorized investigations or related activities and requires Constitutional adherence.

State, local, tribal and territorial public safety partners can model their own internal UAS policy after this Justice Department update. It is important internal UAS policy address laws protecting individual privacy and civil liberties laws as well as airspace rules and regulations.

One important change since the original 2015 policy: the update requires UAS acquisitions to be evaluated for cybersecurity risks. This helps protect public safety entities from potential threats and mirrors other federal agencies' concerns about UAS of foreign manufacture (PDF, 1 MB).

The Justice Department promotes public safety UAS use in appropriate, responsible and effective ways to include:

- Crime scene response.
- Search and rescue.
- Site security.
- Crime investigations.

### 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**



For more information on the safe operation of UAS, see the Federal Aviation Administration website for public safety.

(Source: DOJ)

## Make a resolution to get your family ready for disasters this year

It's still the beginning of the year, relatively, and not too late to start a New Year's resolution. While getting healthy, getting rid of piles of stuff or finally traveling like you've been meaning to are all worthy goals, why not tackle something most of us preach regularly but never do ourselves: prepare yourself and your family for disasters and emergencies.

First responders can get called out at a moment's notice at any hour of the day. Sometimes the emergency is a flood, hurricane or wildfire affecting your own family or home. Getting your family prepared enables you to do your job without quite so much added worry.

A few simple steps can go a long way to ensuring your family's safety. Ready.gov's webpage "Ready Responder" offers resources and guides for both firefighters and law enforcement to help with this goal. The site also offers these tips:

- Create evacuation plans, both escape plans to get everyone out of a residence in case of fire as well as evacuation plans in the event of a larger disaster. Have multiples of each plan.
- Designate emergency contacts, preferably someone out-of-town, that your family members will contact once they are safe.
- Make go-bags for everyone in the house and one for pets.
- Practice! Practice all evacuation and escape plans and make changes as necessary.

(Source: Ready.gov)

## Newly revised Executive Fire Officer program application period open

The application period for the newly revised Executive Fire Officer (EFO) program at the National Fire Academy is currently open and will close on April 15, 2020. The EFO program provides senior officers enhanced knowledge on management and leadership problems facing fire and EMS departments.

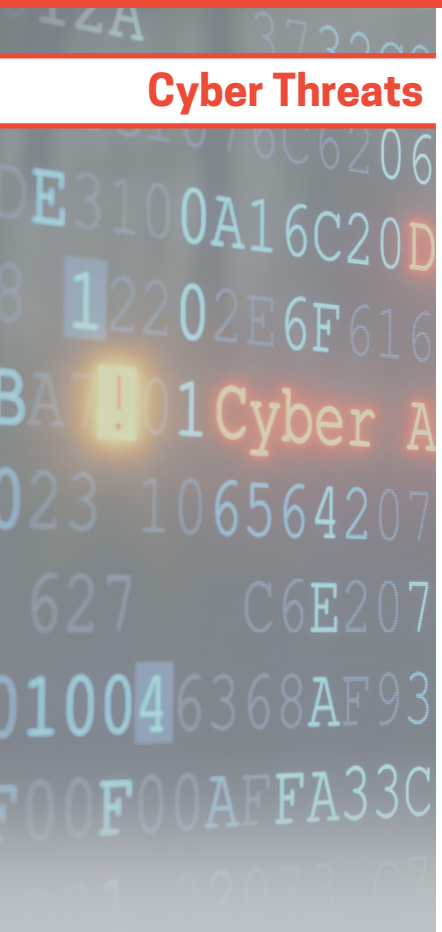
EFO is moving from a 4-year program to 2 years, blending online learning with on-campus courses. Students will be grouped into cohorts and move through the program together, finishing up with individual graduate-level thesis projects.

See the EFO webpage on the U.S. Fire Administration website for admission requirements and details on how to apply.

Each year, NFA hosts the EFO Program Symposium, a networking, education and information sharing opportunity for EFO graduates and other fire service exeutives and colleagues in government management. The 2020 Symposium is scheduled for April 17-18. See the symposium website for a list of the individual and organizational presentations. Symposium registration closes March 15, 2020.

(Source: USFA)

## Cyber Threats



### New Ryuk info stealer targets government and military secrets

A new version of the Ryuk Stealer malware has been enhanced to allow it to steal a greater amount of confidential files related to the military, government, financial statements, banking and other sensitive data.

It is not known if this tool is created by the Ryuk Ransomware actors to be used for data exfiltration before encrypting a victim's computer or if another actor simply borrowed from the ransomware's code.

What we do know is that **the malware is targeting very specific keywords that could be disastrous for governments, military operations and law enforcement cases** if the stolen files are exposed.

(Source: Bleeping Computer)

### Phishing today, deepfakes tomorrow - training employees to spot them

With the sheer amount of jobs requiring their employees to be online, it's critical that workforces are educated and provided with the tools to detect, refute and protect against deepfake attacks and fraudulent activity taking place in the workplace. It's not difficult to see why corporate deepfake detection in particular is so crucial: employees by nature are often eager to satisfy the requests of their seniors, and do so with as little friction as possible.

**Companies must empower employees to question and challenge requests that are deemed to be unusual**, either because of the atypical action demanded or the out-of-character manner or style of the person making the request. This can be particularly challenging for organizations with very hierarchical and autocratic leadership that does not encourage or respect what it perceives as challenges to its authority.

(Source: Dark Reading)

### Developing a cyber breach public relations plan

In the digitally connected age we live in, our data is everywhere, making it possible for even the likes of the CIA to get hacked. When arguably the most secure organization in the world can be cyber breached, it's safe to say the probability of a cyber breach happening to a regular company is pretty high, and the impacts could be devastating.

Damages to an organization as a result of cybercrime (e.g., loss of revenue, stolen data or money, compliance fines, lawsuits, data restoration services) can be scary, but in my experience of speaking to executives about these very concerns, the biggest fear of a cyber breach is the damage to a company's brand, resulting in a loss of trust with clients, partners and employees.

That being said, if we know there is a high probability of a cyber breach to come our way, and among our main concerns is what that breach will do to our brand, then **as we build a strategy of how to respond to a breach, we need to include within that strategy a cyber breach public relations plan**.

(Source: Forbes)

### 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.