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

The InfoGram

Volume 20 — Issue 2 | January 9, 2020

Updated NTAS Bulletin covers changed threat landscape after airstrike

The Department of Homeland Security (DHS) issued a new National Terrorism Advisory System (NTAS) Bulletin on January 4, 2020. The bulletin pertains to the changing threat landscape following the United States-led airstrike in Iraq.

There are currently no specific, credible threats against the homeland; however, Iranian leaders have promised retaliation against the United States and its allies for this attack. DHS also states homegrown violent extremists may use current events to their advantage.

All first responders, all levels of government and private stakeholders should strongly consider operating under an enhanced posture to improve coordination and situational awareness should any specific threats emerge.

In addition to a history of physical acts of violence, Iran has a very strong cyber program and is able to carry out cyberattacks against the United States. If your agency has not yet bolstered its cyber posture, now is the time. The Cybersecurity and Infrastructure Security Agency (CISA) published a bulletin this week detailing Iran's overall threat profile. There are already reports of a significant uptick in hacking attempts originating in Iran.

Everyone within your organization should know how to recognize suspicious activity affecting both physical security and cybersecurity, who it should be reported to and where to go for more information. Good online resources include DHS's Hometown Security Campaign, the Ready.gov website and CISA.

The Nationwide Suspicious Activity Reporting (SAR) Initiative offers free online SAR training for fire/EMS personnel, law enforcement public health and healthcare partners, emergency managers and public safety telecommunicators.

(Source: DHS)

Wear Blue day brings increased awareness to human trafficking

January is Human Trafficking Awareness Month. Blue Campaign national public awareness campaign is designed to educate the public, law enforcement and other industry partners to both recognize indicators of human trafficking and know how to respond to suspected cases.

Reporting indicators of trafficking is the first step to getting someone out of a horrible situation. It could even save their life. First responders are in a great position to spot the signs of human trafficking. Earlier this year, the U.S. Fire Administration produced an awareness video to educate fire and EMS personnel. Fire department leadership should consider using the short video to train personnel.

Blue Campaign hosts several events and educational activities throughout January. This weekend is the Blue Campaign's largest initiative: #WearBlueDay on January 11.

To raise awareness of human trafficking, people may take photos of themselves, friends, family and colleagues wearing blue clothing and share them on social media – Facebook, Twitter, Instagram – along with the #WearBlueDay hashtag. Anyone can participate, all you need is a piece of blue clothing!

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

Follow the campaign on Twitter @DHSBlueCampaign for more information on #WearBlueDay and National Human Trafficking Awareness Day.

The Blue Campaign offers law enforcement, fire and EMS personnel free training and information on how to identify and report possible victims of human trafficking. Visit the website for more resources. There is also a victim identification handout available in multiple languages.

(Source: DHS)

FEMA upgrades Integrated Public Alert and Warning System (IPAWS)

The Federal Emergency Management Agency (FEMA) recently integrated updates to the Integrated Public Alert and Warning System (IPAWS), improving Wireless Emergency Alerts (WEA) and giving authorities more capabilities when sending to cellular phones and other wireless devices.

The updates include Spanish-language capabilities, an increase from 90 to 360 characters per message and an expanded alert category allowing the public to opt-in to a test message category for state and local officials. The updates also include more accurate geo-targeting capabilities for alerts. Television and radio alerts via the Emergency Alert System are not affected by this upgrade.

The enhancements require updates to wireless provider networks across the nation and updates to customer phones. All updates are being coordinated with the Federal Communications Commission.

(Source: FEMA)

Webinar: North Bay Wildfires, lessons learned from REDCOM Dispatch

An upcoming International Public Safety Association (IPSA) webinar will cover the experiences of the Redwood Dispatch Communications Authority (REDCOM) team in managing what were at the time the most destructive wildfires in California history.

The webinar will provide facts about the incident, discuss lessons learned, how they managed their own internal emergencies and how they plan to move forward after the Tubbs, Nuns, and Pocket fires destroyed 7,000 homes and business and killed 24 in Sonoma County on October 8, 2017.

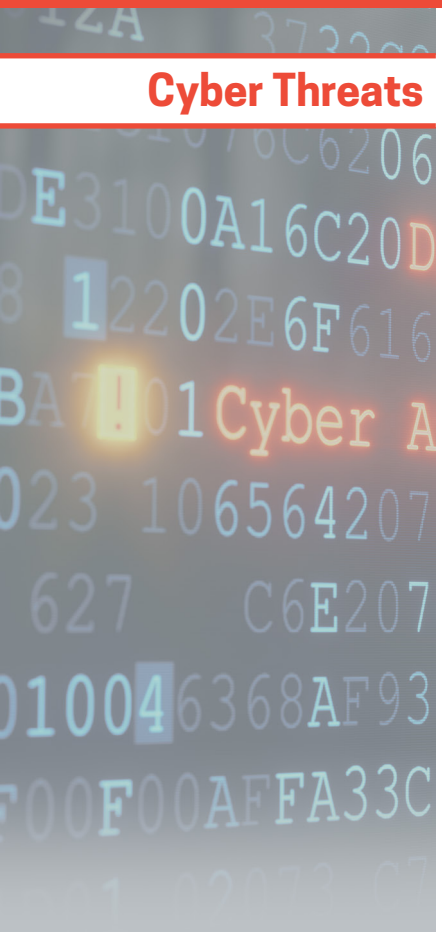
The webinar is scheduled for Wednesday, January 29, 2020, from 1-2:15 p.m. Eastern. Registration is required, the webinar is free.

Descriptions of the sessions:

- Overview of REDCOM Dispatch as a Consolidated Fire and EMS Dispatch Center
- Overview of the Tubbs, Nuns, and Pocket Fires
- Dispatch Perspective of the incident management
- Pitfalls in emergency notifications/Wireless Emergency Alerts
- Managing internal emergencies
- Medical Facility Evacuation Details and Methods
- Peer Support
- Objectives Moving Forward

(Source: IPSA)

Cyber Threats



Windows 7 end of life: what are your options?

Are you a Windows 7 user? Come January 14, 2020, Microsoft will no longer provide security or support for the Windows 7 and Windows Server 2008/R2 operating systems, meaning patching and technical support via Microsoft's support center will no longer be available.

That means **continuing to use either operating system after this date will put your system at risk of attack from new, unpatched vulnerabilities**. Running your business on an outdated (and unsupported) system is a huge security risk.

(Source: FBI)

Russia successfully disconnects from global Internet in test

Russia has run a successful test of a country-wide alternative to the global Internet, according to BBC News.

While details of the test are vague, Russia's defense ministry of communications reportedly said that regular users did not notice any obvious changes to their Internet access. The results of the test are expected to be sent to Russian President Vladimir Putin for review.

BBC News noted that other countries including Iran and China have made similar moves in creating their own alternative system to the global Internet.

(Source: The Hill)

Your car may be vulnerable to attack, even the smartest ones

The emergence of smart cars has opened the door to limitless possibilities for technology and innovation – but also to threats beyond the car itself. New research from Michigan State University is the first to apply criminal justice theory to smart vehicles, revealing cracks in the current system leading to potential cyber risks.

As vehicles become smarter and more connected to WiFi networks, hackers will have more opportunities to breach vehicle systems. **Connecting your smartphone through a USB port can give a hacker backdoor access to data from both your phone and your car**. Additionally, Google Android users who can download apps from unverified sites are even more at-risk.

(Source: SciTechDaily)

Password-stealing hacking campaign targets government agencies

A mysterious **new phishing campaign is targeting government departments and related business services around the world** in cyberattacks aiming to steal login credentials from victims. In total, the phishing attacks have targeted at least 22 different organizations in countries including the United States, Canada, China, Australia, Sweden and more.

All of the attacks involve emails claiming to be related to the targeted government agencies and all of them attempt to trick victims into clicking an email link that asks for their username and password. Anyone who enters their login credentials into the spoofed government agency websites will give cyber criminals access to their account.

(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.