EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

The InfoGram

Volume 17 – Issue 20 *May 18, 2017*

Highlights:

The U.S. Fire Administration maintains 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.**

Officer Brushes Powder Off Uniform, Nearly Dies

A police officer in Ohio responded to a traffic stop that turned out to also be drug-related with fentanyl powder all through the vehicle. Officers donned protective gloves and masks, which is a recommended practice now with fentanyl on the rise. However, when he got back to the station, he brushed something off his shirt.

Within minutes he was on the floor, his body shutting down. Paramedics who were at the station treating one of the arrested men from the original call treated the officer with Narcan to stop the overdose. If the officer had brushed the powder off his uniform in his car on his way home, he likely would have died. If he had gotten home before noticing it, his family could have come into contact with it.

Drug and medical officials have issued warnings about this possibility for months. Law enforcement, EMS, and fire personnel are strongly encouraged to wear protective gear at emergencies or crime scenes where fentanyl may be present. Please see the Drug Enforcement Agency's Roll Call video on officer safety and fentanyl, and read "Fentanyl: Incapacitating Agent," by the Centers for Disease Control and Prevention.

(Source: CDC)

New NTAS Bulletin Focus on Homegrown Threats

The Department of Homeland Security (DHS) issued a new National Terrorism Advisory System (NTAS) Bulletin earlier this week. The new bulletin again focuses on homegrown violent extremists, updating the information released in the expired November 2016 NTAS bulletin.

This bulletin aims to increase the public's knowledge and understanding of threats facing the United States, including attacks using vehicle ramming, small arms, straight-edged blade, and homemade explosives. These tactics have been used in Europe over the past few years with varied success. The updated bulletin lists who to contact to report suspicious activity, what to prepare, and how to stay informed.

The NTAS system has three levels of advisories: a general bulletin, an elevated alert, and an imminent alert. Since its revision in 2015, only bulletins have been issued.

(Source: NTAS)

Cyberattack Hits Critical Infrastructure Worldwide

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

A major worldwide ransomware attack hit critical infrastructure and government computers starting late last week, prompting warnings, patches, and other support to those that may have already been infected or who may be looking to prevent infection. Affected industries worldwide include healthcare, railway operations, mail delivery, government offices, schools, and factories. This is the largest ransomware infection in history.

CNET reports over 100,000 organizations were affected in 150 countries, including the United States. This attack spread rapidly and infected hundreds of thousands of systems. Ransomware attacks hold systems and data in exchange for a payment. In this case, the attackers are demanding approximately $200-$300 to unlock each system. Media reports the attackers could make over $1 billion.

Three very basic things can keep your networks clear:

- **Do not** click on links in emails or download files attached to emails unless you are expecting them and have verified their authenticity;
- **Install software patches or updates** on all personal and work devices;
- **Back up your data!**

If your data is properly and regularly backed up, an attack like this won't pose as much of a problem. The devices and network can be wiped clean and the backed up data can be restored. The key is to update often and regularly, even daily or several times a day right now as we know this attack is rampant.

For more information on this attack and how to protect your organizational and personal devices, visit the United States Computer Emergency Readiness Team (US-CERT) for regular updates. The FBI and DHS published an alert listing indicators of the ransomware (PDF, 190 Kb). The interagency report "How to Protect Your Networks from Ransomware" (PDF, 631 Kb) provides best practices and mitigation strategies for prevention and response HelpNetSecurity also has a guide on protecting systems from ransomware with actions ranging from the technical level to the human level.

If you suspect a cyberattack, contact your state police or regional FBI Field Office.

(Source: US-CERT)

National Information Sharing Consortium Webinar

On June 1st, the National Information Sharing Consortium will host a webinar with the DHS's Emergency Services Sector-Specific Agency (ESS) on resources and tools available to the first responder community. Covered topics include:

- ESS Resilience Development Project;
- ESS Roadmap to Secure Voice and Data Systems;
- ESS-Specific Tabletop Exercise Program (ES SSTEP);
- ESS Cybersecurity Initiative;
- ESS Resilience Development Webinar Series.

This is the second DHS ESS webinar in the NISC's Mission-Focused Job Aids Webinar Series. The series reviews tools, techniques, and standard operating procedures for NISC partners in the homeland security, emergency management, public safety, first responder, and healthcare preparedness communities to use to facilitate and manage information sharing.

For more information about the webinars series and NISC, visit the NISC website. NISC membership is free for all users.

(Source: NISC)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local *FBI office* and also the *State or Major Urban Area Fusion Center*.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.