INFOGRAM 16-12   April 18, 2012

NOTE: This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@fema.dhs.gov.

Cyber Attacks on Critical Infrastructure and 9-1-1
(Source: Homeland Security Newswire and ICS-CERT)

Industrial Control Systems (ICS) used to manage chemical, water, and energy systems are dealing with an increase of cyber attacks, according to an article published earlier this month in Homeland Security Newswire. Attacks are occurring on a daily basis and are usually denial-of-service or cyber espionage in nature.

In many cases, attackers are using a kind of social engineering known as spear-phishing. Spear-phishing is when an individual receives an email with a link from what looks like a trusted source. If the link is clicked, malware will be downloaded to conduct cyber espionage. An example of this is detailed in a Symantec report about 2011 cyber attacks on the chemical industry.

In addition to utilities, cyber security has become more of an issue for radio communications within the 9-1-1 and dispatching systems. Many Public Safety Answering Point (PSAP) communication systems are now using internet protocol (IP), as opposed to older radio-based systems. Urgent Communications magazine began a series of articles about this subject. In the March 2012 article, they describe a few of the problems facing the industry as well as the results of a survey to their readership regarding the issues of cyber security.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) found that Department of Homeland Security's ICS Cyber Emergency Response Team (ICS-CERT) offers assistance to critical infrastructure asset owners on how to better prepare networks and people to deal with and analyze a cyber incident. Their online Overview of Cyber Vulnerabilities describes the many varieties of cyber attacks and weaknesses that exist. Their services include response to incidents, analysis of vulnerabilities, and sharing situational awareness information and threat analysis.

Federal Excess Personal Property (FEPP) Program
(Source: U.S. Forest Service Fire & Aviation Management)

Every year, the U.S. Forest Service Fire and Aviation Management Program loans millions of dollars worth of excess federal property to state foresters through the Federal Excess Personal Property (FEPP) program. The majority of excess property is then sub-loaned to local or rural fire departments for the purpose of enhancing wildland fighting.

The FEPP website explains: "the State Forester makes the initial decision that a FEPP item is appropriate for use, and the USDA Forest Service must concur. The property is then loaned to the State Forester, who may then place it with local departments to improve local fire programs." Receivers of FEPP property need only have wildland or rural fire duties that satisfy the State Forester.

According to the program's Frequently Asked Questions page, excess property can include apparatus, tanks, hoses, even motor oil and other vehicle maintenance items, but not real estate or buildings. Most often, the vehicles available are military trucks or other general-purpose vehicles, not fire apparatus, and they require rehabilitation to be used as firefighting equipment.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) sees from the success stories page that the program is not just geared toward states that are well known for their wildfire and forest fire dangers. Contact your state's forestry coordinator or regional Forest Service FEPP Manager for more information on the program.

Best Practices for Emergency Vehicle Visibility Study
(Source: USFA)

A new study on emergency vehicle visibility during roadway operations is underway with the goal of reducing emergency vehicle crashes and enhancing responder safety. The study was initiated by the U.S. Fire Administration (USFA), supported by the U.S. Department of Justice National Institute of Justice, and is through a partnership with the Cumberland Valley Volunteer Firemen's Association Emergency Responder Safety Institute.

Quoting the press release, "The goal of this study is to develop best practices in the application of various chevron patterns, creative use of reflective decal markings, new arrangements of warning lights, and other innovative designs – all with the intent of increasing the visibility of the emergency vehicles to motorist approaching them."

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) found more information on the emergency vehicle and roadway safety research initiatives section of the USFA website.

Carbon Monoxide Poisoning Prevention Toolkit
(Source: CDC)

Another early start to tornado season and hurricane season officially starting June 1 brings carbon monoxide poisoning during disasters to the forefront again due to the use of portable gasoline-powered generators. The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned from the Centers for Disease Control and Prevention's (CDC) Carbon Monoxide FAQ page that at least 20,000 people seek emergency medical treatment and hundreds of people in the United States die every year from carbon monoxide (CO) poisoning accidents.

Several helpful resources are now available for emergency managers and public health officials, including the CDC's "Carbon Monoxide Poisoning Prevention: A Toolkit." Recently published, the toolkit comes complete with public safety campaign flyers and bill inserts for energy companies.

The National Institute of Standards and Technology (NIST) posted a short informational video on YouTube called "How Close is Too Close for Portable Generators?" The video gives a brief description of testing done by NIST and the CDC and provides a few guidelines, including a reminder to place and maintain CO detectors near sleeping areas.

DISCLAIMER OF ENDORSEMENT

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

REPORTING NOTICE

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. FBI phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm*. Fusion Center information can be seen at* http://www.dhs.gov/contact-fusion-centers*.*

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*.*

When available, each report submitted should include the date, time, location, type of activity, number of people, equipment used for the activity, name of submitting person and organization, and a designated point of contact.