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

The InfoGram

Volume 16 – Issue 18 May 5, 2016

NIOSH Warns of Counterfeit Respirators

The National Institute for Occupational Safety and Health (NIOSH) is warning the industry about counterfeit respirators on the market. According to the notice, a manufacturer is selling N95 respirators and marketing them as NIOSH-approved despite not being a NIOSH approval holder or a private label holder.

Several other manufacturers have had their NIOSH-approval status rescinded in the past several years and are misrepresenting their products. NIOSH has contacted all of these manufacturers to rectify the situation.

To check the status of the respirators your department or agency uses and ensure they are NIOSH-approved, use their searchable Certified Equipment List to find them. You may also familiarize yourself with the required exterior markings on approved respirators using the guide and pictures at the bottom of NIOSH's Respirator User Notices page and the Respirator Trusted-Source Information page.

(Source: NIOSH)

Ransomware Still Targeting Law Enforcement

Ransomware attacks against various sectors is still going strong, and law enforcement agencies are right up there as ransomware targets. A virus is inadvertently downloaded onto departmental networks, locking the system and encrypting files. Hackers hold the files hostage until the victim pay the ransom using digital currency, which can be in the hundreds or thousands of dollars. If the ransom is not paid, hackers may delete the files, which happened to police departments at least twice last year, affecting cases and collected, stored evidence.

The good news is most of the time simply educating employees and officers on what to look for in suspicious emails will keep ransomware off of your systems (PDF, 759 Kb). Ransomware infects computers when someone clicks on a link or an attachment in an email that looks legitimate – such as a digital fax or invoice. Opening the attachment or link infects the computer and spreads to the network.

The key here is teaching and reminding employees to be sure the email is from a legitimate source and the attachment or link is what it claims to be. If there is any question at all, don't open the link or attachment and double-check with the sender, or simply delete the message. If it is legitimate and that important, they will send it again or call if they didn't hear from you.

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

Highlights:

NIOSH Warns of Counterfeit Respirators

Ransomaware Still Targeting Law Enforcement

USFA: New Wildland Urban Interface Toolkit

2016 Emergency Response Guidebook Released

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.

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.**

It is also important to back up files and data on a regular basis and not to store the back up on the main network, which would defeat the purpose. Up-to-date virus protection is also a must. Both of these things can be accomplished for a reasonable fee and time investment and will pay off if and when your department turns out to be the next ransomware target.

(Source: Government Technology)

USFA: New Wildland Urban Interface Toolkit

Wildfire season is upon us already. Fire activity in the United States is picking up and over 88,000 residents of Fort McMurray in Alberta, Canada, were forced to evacuate as a fast-moving fire has already destroyed an estimated 1,600 buildings and may destroy the city.

Last week, the U.S. Fire Administration (USFA) released the Wildland Urban Interface (WUI) Toolkit. The collection contains:

- Outreach materials – information on organizations that focus on creating fire adapted communities, such as Firewise and Ready, Set, Go!
- Codes and Standards – links to the International WUI Code and the National Fire Protection Association's codes;
- Assessment Tools – things both residents and the fire service can take stock of to determine the community's risk;
- Research – current research on WUI and wildfires;
- Training – links to training for members of the community.

This collection of recommended resources will assist fire departments, community organizations, local governments, emergency managers, and citizens alike to strengthen the way their city or town prepares for a wildfire emergency.

(Source: USFA)

2016 Emergency Response Guidebook Released

The Pipeline and Hazardous Materials Safety Administration (PHMSA) has announced the release of the 2016 Emergency Response Guidebook (ERG). The ERG is updated every four years and gives first responders detailed information on hazardous materials to better manage accident or spill response during the critical early stages of an incident.

Jointly developed with the governments of Canada and Mexico, the Department of Transportation wants to have a copy in every public emergency service vehicle in the country. The 2016 ERG has a table of initial isolation and protective action distances, added guide pages for absorbed gases, and other things as listed on this Summary of Changes (PDF, 1 Mb).

The ERG is available through many outlets for purchase; however, PHMSA will be distributing over 1.5 million free copies directly to fire, EMS, and law enforcement agencies and departments around the country. Contact your state's ERG distribution coordinator (PDF, 113.5 Kb) for more information. A copy is also available free online, and will be developed as a free smartphone app to replace the ERG2012 version currently available.

(Source: PHMSA)

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes 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.

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**.