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

The InfoGram

Volume 20 — Issue 29 | July 16, 2020

FDA adds to the list of dangerous hand sanitizers containing methanol

In late June, the Food and Drug Administration (FDA) issued a warning on the presence of toxic chemicals in some brands of hand sanitizer. The FDA recently added more brands and products to the list of methanol-contaminated hand sanitizers.

The FDA reports adults and children are ingesting hand sanitizer products contaminated with methanol. The agency has seen a sharp increase in hand sanitizer products labeled to contain ethanol (also known as ethyl alcohol) but that have tested positive for methanol contamination.

Methanol is not an acceptable active ingredient for hand sanitizers and must not be used due to its toxic effects. FDA's investigation of methanol in certain hand sanitizers is ongoing.

No one should use any products on this list of hand sanitizers with potential methanol contamination, and you should continue checking the list often as it is being updated daily.

EMS personnel should be aware that people are ingesting hand sanitizer and be prepared to manage such cases. These incidents have led to blindness, hospitalizations and death in patients. Substantial methanol exposure can result in nausea, vomiting, headache, blurred vision, permanent blindness, seizures, coma, permanent damage to the nervous system or death.

Although all persons using these products on their hands are at risk for methanol poisoning, young children who accidently ingest these products and adolescents and adults who drink these products as an alcohol (ethanol) substitute are most at risk.

The agency will provide additional information as it becomes available.

(Source: FDA)

Risks of counterfeit PPE, how to identify them, how to report them

Sales and production of fraudulent PPE – especially N95 and KN95 masks – have increased since December 2019 as people took advantage of the pandemic to make some money. Many agencies and departments are having problems getting PPE and have to source from unknown sellers. It's important to be able to identify fraudulent, counterfeit or unapproved products in order to ensure the safety of your personnel.

A new fact sheet from the Technical Research, Assistance Center, Information Exchange (TRACIE) provides a quick reference to help you protect your staff with safe, approved PPE and instructions on how to report sellers of counterfeit products.

Respirators for Healthcare during COVID-19: Authorized Use and Avoiding Fraudulent Products recommends the National Institute for Occupational Safety and Health (NIOSH) Certified Equipment List and the Food and Drug Administration's Emergency Use Authorization list. These lists give you information on what types of masks or respirators are to be used under what circumstances, use of imported products and indicators of counterfeit products and vendors.

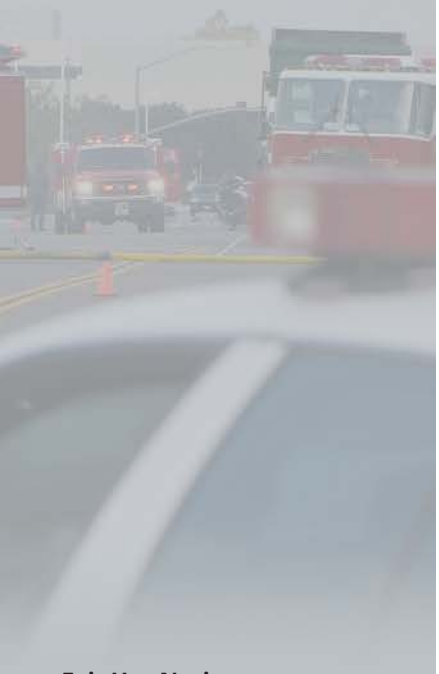
Highlights

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



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.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Review this guidance and consider keeping it on-hand as a reference to help ensure the safety of people in your department.

(Source: ASPR TRACIE)

FEMA releases updated public assistance guidance

The Federal Emergency Management Agency (FEMA) released the fact sheet Coordinating Public Assistance and Other Sources of Federal Funding to provide clear guidance on how FEMA will treat the multiple sources of funding as they relate to the public assistance program and its cost share requirements.

To respond to the coronavirus (COVID-19) pandemic, Congress authorized more than $3 trillion to multiple federal agencies to provide assistance to state, local, tribal and territorial governments. Several agencies are offering aid and in some cases it overlaps with FEMA authority. Generally, funding from other federal agencies cannot be used to meet the FEMA public assistance non-federal cost share requirement.

For COVID-19, however, there are two exceptions: Department of Treasury's Coronavirus Aid, Relief, and Economic Security (CARES) Act Relief Fund and the Department of Housing and Urban Development's Community Disaster Block Grant (CDBG-CV). While cost share requirements vary from agency-to-agency and program-to-program, many programs funded by the CARES Act and the other supplemental appropriations do not require a non-federal share.

(Source: FEMA)

New industrial control system security 5-year strategy released

The Cybersecurity and Infrastructure Security Agency (CISA) published Securing Industrial Control Systems: A Unified Initiative. This 5-year strategy provides a framework and guidance to strengthen and unify industrial control systems (ICS) cybersecurity to better protect the essential services provided daily.

CISA will work with critical infrastructure owners and operators – and the whole ICS community – to build ICS security capabilities directly empowering stakeholders to secure their operations against ICS threats. They will also work to improve CISA's ability to anticipate, prioritize and manage risk by supporting national efforts to secure control systems in the areas of workforce development, standards and best practices, supply chain risk management, and incident management.

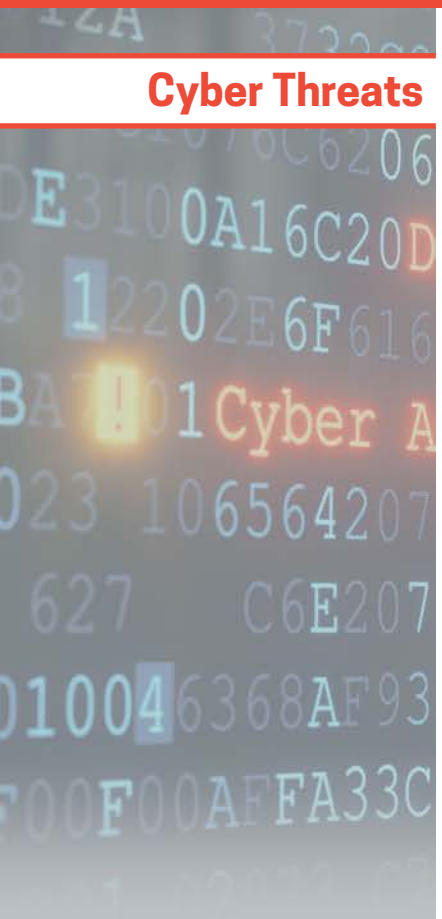
The initiative builds around four pillars:

- Pillar 1: Ask more of the ICS Community, deliver more to them.
- Pillar 2: Develop and utilize technology to mature collective ICS cyber defense.
- Pillar 3: Build "deep data" capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS cyber kill chain.
- Pillar 4: Enable informed and proactive security investments by understanding and anticipating ICS risk.

CISA is striving to move the ICS community beyond reactive measures to a more proactive, unified ICS security focus. Contact CISA at central@cisa.gov for more information about services CISA provides to ICS stakeholders.

(Source: CISA)

Cyber Threats



Pipeline Cybersecurity Initiative

The Cybersecurity and Infrastructure Security Agency (CISA) is working with government and industry partners to identify cybersecurity risks and develop strategies to strengthen the nation's pipeline infrastructure.

Through the Pipeline Cybersecurity Initiative (PCI), CISA, in coordination with the Transportation Security Administration (TSA) and other federal and private sector partners, is working to develop a better understanding of cybersecurity risk across the pipeline infrastructure. By identifying vulnerabilities within the information technology (IT) and operational technology (OT) systems, the initiative is helping pipeline owners and operators harden their cybersecurity posture.

In support of this effort, CISA and TSA has published Pipeline Cyber Risk Mitigation Infographic to outline activities pipeline owners and operators can use to improve their ability to prepare for, respond to and mitigate against malicious cyber threats.

(Source: CISA)

Monthly cybersecurity webinars continue for HPH sector

The Health Sector Cybersecurity Coordination Center (HC3) will continue hosting monthly webinars in its threat briefing series to discuss actionable cybersecurity threats and mitigation practices for the Healthcare and Public Health (HPH) sector.

The next briefing covering "Dark Web and Cybercrime Deep Dive" is scheduled for Thursday July 23, 2020, at 1 p.m. Eastern and subsequent briefings will be hosted on a monthly basis. These unclassified briefings are open to professionals in the healthcare industry with a range of backgrounds and expertise in cybersecurity.

To receive the webinar meeting details, and for more information, please contact HC3@hhs.gov.

(Source: HC3)

FBI sees spike in fraudulent unemployment insurance claims

The FBI has seen a spike in fraudulent unemployment insurance claims complaints related to the ongoing COVID-19 pandemic. Citizens from several states have been victimized by criminal actors impersonating the victims and using the victims' stolen identities to submit fraudulent unemployment insurance claims online.

Criminals obtain a stolen identity using a variety of techniques, including the online purchase of stolen personally identifiable information (PII), previous data breaches, computer intrusions, cold-calling victims while using impersonation scams, email phishing schemes, physical theft of data from individuals or third parties, and from public websites and social media accounts, among other methods.

Many victims of identity theft related to unemployment insurance claims do not know they have been targeted until they try to file a claim for unemployment insurance benefits, receive a notification from the state unemployment insurance agency, receive an IRS Form 1099-G showing the benefits collected from unemployment insurance, or get notified by their employer that a claim has been filed while the victim is still employed.

(Source: FBI)

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.