U.S. Fire Administration | FEMA

EMR-ISAC InfoGram July 15 - DHS S&T showcases research and technology for resilience; FDA no longer authorizes use of non-NIOSH-approved or decontaminated disposable respirators

EMR-ISAC sent this bulletin at 07/15/2021 03:30 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 21 — Issue 28 | July 15, 2021

FDA no longer authorizes use of non-NIOSH-approved or decontaminated disposable respirators

On June 30, the FDA announced the revocation of Emergency Use Authorizations (EUAs) for imported, non-NIOSH-approved respirators as well as decontamination and bioburden reduction systems. This impacts all health care personnel, including emergency medical services personnel. The revocation of these EUAs was due to the increase in domestically manufactured, NIOSH-approved N95s available throughout the country.

On April 9, the U.S. Food and Drug Administration (FDA) issued a letter to health care personnel and facilities, recommending a transition away from crisis capacity conservation strategies, such as decontaminating disposable respirators for reuse.

Early in the public health emergency, there was a need to issue EUAs for non-NIOSH-approved respirators as well as decontamination and bioburden reduction systems to disinfect disposable respirators.

Those conditions no longer exist. Since the beginning of the pandemic, NIOSH has approved more than 875 respirator models or configurations, with some of these manufactured by approximately 20 new, domestic NIOSH-approval holders. There are now more than 6,400 total respirator models or configurations on the NIOSH-certified equipment list.

Highlights

The FDA recommends that health care agencies consider redistributing current inventory of non-NIOSH-approved respirators to non-health care settings for non-medical use (for example, construction), and to other countries in need.

The FDA also recommends agencies increase inventory of available NIOSH-approved respirators, including:

- N95s and other disposable filtering facepiece respirators (FFRs).
- Elastomeric respirators, including new elastomeric respirators without an exhalation valve that can be used in an operating room.
- Powered air-purifying respirators (PAPRs).

If you have questions about respirators or decontamination systems, you can contact the U.S. Food and Drug Administration's Division of Industry and Consumer Education (DICE). DICE develops educational resources for the FDA website to help the medical device industry understand FDA regulations and policies.

(Source: FDA)

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 fema-emr-isac@fema.dhs.gov.

Subscribe here

DHS S&T showcases research and technology for resilience against pandemics, natural disasters and threats

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has convened U.S. government (USG) research organizations to showcase research and development accomplishments through their four-part series, Whole-of-Government Virtual R&D Showcase. The theme, "Unifying Research to Work for You," addresses how DHS S&T and its partners are moving research from the lab into the world.

The Whole-of-Government Virtual R&D Showcase demonstrates how USG researchers are addressing challenges facing our critical infrastructure and lifeline services. Topics cover cross-sector collaborations in the following areas: COVID-19 threat characterization and assessment, disaster resilience, evolving threats, safeguarding public transit, virus detection, drone operations, aviation security, and the convergence of advanced technologies.

The four series in the Showcase are:

- Series 1, Enhancing Public Health Security and Resilience.
- Series 2, Building Resilience and Innovation Equity.
- Series 3, Mitigating Evolving Threats and Understanding the Convergence of Breakthrough Technologies.
- Series 4, Building Whole-of-Government R&D Partnerships.

Each series features several expert panel discussion videos, an e-book, and additional resources

related to the series topic. Series 1 and 2 are now available. Series 3 and 4 will become available on July 26 and August 9, respectively, when exclusive content is unlocked on those dates.

This event is free and there is no registration required. All content for each series will be available on the site until November 2021.

To learn more, see the Whole-of-Government Virtual R&D Showcase informational flyer and website. You can also follow DHS S&T on Twitter at @DHSSciTech for news and announcements.

(Source: DHS S&T)

FEMA webinar series on competitive Hazard Mitigation Assistance grant programs

The Federal Emergency Management Agency (FEMA) is hosting a webinar series this summer, beginning late July through October, to provide information and guidance on two competitive Hazard Mitigation Assistance grant programs:

- The Building Resilient Infrastructure and Communities (BRIC) Program.
- The Flood Mitigation Assistance (FMA) Program.

BRIC is a new program that replaces FEMA's existing Pre-Disaster Mitigation (PDM) program. Through BRIC, FEMA continues to invest in a variety of mitigation activities with an added focus on infrastructure projects and Community Lifelines. The program encourages the adoption and enforcement of modern building codes.

The FMA program funds projects that reduce or eliminate the risk of repetitive flood damage to buildings and structures insured by the National Flood Insurance Program. The FMA grant program strengthens national preparedness and resilience and supports the mitigation mission area through FEMA's strategic goal of building a culture of preparedness.

The target audience for this webinar series are leaders in state, local, tribal and territorial (SLTT) agencies, as well as private sector and non-profit organizations.

The webinars in the series cover technical information, best practices, tools and resources regarding these grant programs. FEMA subject-matter experts are available during some sessions to answer questions from applicants.

To attend any of these webinars, visit FEMA's website for a schedule and links to register. All sessions will be recorded and posted to FEMA's YouTube channel.

(Source: FEMA)

EMI releases 2022 schedule for Virtual Tabletop Exercise Program

The Federal Emergency Management Agency's (FEMA's) Emergency Management Institute (EMI) has released its 2022 schedule for the Virtual Tabletop Exercise (VTTX) Program. VTTX offerings this year focus on three of the eight Principals' Strategic Priorities of FEMA's National Exercise Program: 1) Cybersecurity; 2) National Security Emergencies and Catastrophic Incidents; and 3) Operational Coordination and Communication.

Each VTTX is four hours in length and will allow participants to apply the Strategic Priorities to a realistic scenario in a facilitated, no fault, hazard-specific exercise discussion. Scenarios this year include:

- Natural disasters, including flooding, winter weather, earthquakes, hurricanes and more.
- Man-made threats such as active shooters and vehicles as a weapon.
- Planned large gatherings such as sporting events.
- Cybersecurity.

Several VTTX offerings this year will focus on cybersecurity. Cybersecurity VTTXs' are facilitated by the Cybersecurity and Infrastructure Security Agency (CISA). They are based on a current cybersecurity issue and are available in basic, intermediate, and advanced levels.

Each VTTX is designed to leverage the "whole community" concept, with 10 to 15 representatives from participants' local Emergency Management Community of Practice (CoP). For this reason, organizations are encouraged to apply for VTTX training in groups of five or more.

The VTTX Program has made a few changes to its delivery format accommodate the COVID-19 Public Health Emergency. VTTX's are now offered in a completely virtual format using Adobe Connect. Each student will be provided with Adobe Connect information and can participate remotely.

You can learn more about EMI's VTTX Program by visiting EMI's VTTX Program overview. To learn more about EMI's 2022 VTTX offerings and see the full schedule, see EMI's 2022 VTTX Program Bulletin.

If you are interested in conducting a VTTX for your organization, please contact EMI's Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381. Please email at least two weeks in advance of the training event.

For all current training offerings, visit EMI's Training Opportunities and Bulletins page.

(Source: EMI)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

New StopRansomware.gov website – The US government's one-stop location to stop ransomware

The U.S. government launched a new website to help public and private organizations defend against the rise in ransomware cases. StopRansomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts. We encourage organizations to use this new website to understand the threat of ransomware, mitigate risk, and in the event of an attack, know what steps to take next.

The StopRansomware.gov webpage is an interagency resource that provides our partners and stakeholders with ransomware protection, detection, and response guidance that they can use on a single website. This includes ransomware alerts, reports, and resources from CISA, the FBI, and other federal partners.

(Source: CISA)

CISA issues Emergency Directive on Microsoft Windows Print Spooler

CISA has issued Emergency Directive (ED) 21-04: Mitigate

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

CISA has issued Emergency Directive (ED) 21-04: Mitigate Windows Print Spooler Service Vulnerability addressing CVE-2021-34527. Attackers can exploit this vulnerability to remotely execute code with system level privileges enabling a threat actor to quickly compromise the entire identity infrastructure of a targeted organization.

Although ED 21-04 applies to Executive Branch departments and agencies, CISA strongly recommends that state and local governments, private sector organizations, and others review ED 21-04: Mitigate Windows Print Spooler Service Vulnerability for additional mitigation recommendations.

(Source: CISA)

Connecticut becomes third state to incentivize cybersecurity best practices for businesses

The Governor of Connecticut signed HB 6607, "An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses" into law last week. The bill prohibits the Superior Court from assessing punitive damages against an organization that implements reasonable cybersecurity controls, including industry recognized cybersecurity frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the Center for Internet Security (CIS) Critical Security Controls (CIS Controls®).

Connecticut joins Ohio and Utah in legislative efforts to adopt an incentive-based approach for businesses to implement cybersecurity best practices.

(Source: Inside Cybersecurity)

ISAC National Webinar: The Call is Coming from Inside the House – Understanding the Insider Threat

The risks posed by insider threats are not new. In fact, they've represented some of the most powerful storytelling elements in books, movies, folklore, and other media for centuries now.

This presentation will walk through the IT risks posed by insider threats, identify the common technologies and motivations that enable insider threats to be successful, and offer actionable guidance on mitigation and response options. We'll also identify the greatest insider threat movie you've probably already seen.

The webinar will take place on **Tuesday, August 10 at 2:00 p.m. EST**.

(Source: Center for Internet Security)

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