U.S. Fire Administration | FEMA

EMR-ISAC InfoGram Apr. 15 – FDA and NIOSH updates on use of disposable respirators; NASA, Forest Service partnership expands FIRMS active fire mapping capabilities

EMR-ISAC sent this bulletin at 04/15/2021 12:17 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 21 — Issue 15 | April 15, 2021

FDA recommends transition from use of decontaminated disposable respirators, NIOSH updates strategies for optimizing respirator supply

On April 9, 2021, 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. On the same day, the Centers for Disease Control and Prevention's (CDC) National Institute for Occupational Safety and Health (NIOSH) made a corresponding update to its Strategies for Optimizing the Supply of N95 Respirators to clarify how surge capacity strategies should now be applied.

Emergency medical services personnel will be impacted by these recommendations.

The FDA recommendations include:

- Limiting decontamination of disposable respirators.
- Transition away from crisis capacity strategy for respirators, such as decontamination of N95 and other Filtering Facepiece Respirators (FFRs).
- Increase inventory of available NIOSH-approved respirators. Even if you are unable to obtain the

Highlights

respirator model that you would prefer, the FDA recommends that you obtain and use a new respirator before decontaminating or bioburden reducing a preferred disposable respirator.

For more information, read the FDA's Letter to Healthcare Personnel and the updates to CDC NIOSH's Strategies for Optimizing the Supply of N95 Respirators.

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, NIOSH)

NASA, Forest Service partnership expands FIRMS active fire mapping capabilities

The United States Department of Agriculture (USDA) Forest Service's Geospatial Technology and Applications Center (GTAC) announced last month that its Active Fire Mapping Program is migrating to a new web-based platform in 2021, and the legacy Active Fire Mapping website will be decommissioned at the end of the 2021 calendar year.

The new website and map product, Fire Information for Resource Management System (FIRMS) US/Canada, is currently in beta, but available for use as additional capabilities continue to be added.

FIRMS US/Canada is a collaborative effort by the USDA Forest Service and the National Aeronautics and Space Administration (NASA) to provide access to low latency satellite imagery and science data products to support the strategic fire management needs of United States and Canadian agencies, and to inform the general public. It is an expansion on NASA's global FIRMS Fire Map product, which leverages NASA's Earth Observing System (EOS) satellite assets to provide Land, Atmosphere Near Real-time Capability for EOS (LANCE). FIRMS US/Canada, like the original FIRMS product, provides active fire data, generally within three hours of a satellite observation. Imagery is typically also available within three to four hours and can be viewed on an interactive Fire Map application.

So what is new with FIRMS US/Canada? The development of this new instance of FIRMS is tailored to the Forest Service and wildland fire community's active fire mapping needs.

FIRMS US/Canada now meets the new Forest Service requirements with its additional contextual layers and enhancements, such as classification of fires to show time since detection in order to depict active fire fronts, incident locations, and other information for current large fires. It provides current

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

Subscribe here

and other information for current large fires. It provides current and historical corrected reflectance imagery from NASA and National Oceanic and Atmospheric Administration (NOAA) satellites, U.S. and Canada administrative ownership boundaries, daily fire danger forecasts, and current National Weather Service fire weather watch and red flag warning areas.

This information can be utilized by fire managers to assess the current fire situation and serves as a decision support tool in strategic decisions regarding fire suppression resource allocation.

(Sources: NASA, USDA Forest Service)

CARES Act funding for public safety

The CARES Act, which Congress passed in March 2020, provided more than $150 billion for state and local governments to help them respond to greater demand for public services. In December 2020 Congress passed another stimulus bill that extended the deadline for spending this money until December 2021.

Recipients of CARES Act funding have primarily tapped the Department of Justice's Coronavirus Emergency Supplemental Funding Program (CESF) and the Coronavirus Relief Fund (CRF) which funds grants, direct payments and contracts administered by the Federal Emergency Management Agency and other federal, state and county agencies — to address various public safety needs. However, there is a substantial amount of funding remaining.

A recent brief from the Center for Digital Government summarized the variety of possible uses of this remaining funding for public safety.

Coronavirus Relief Fund (CRF) money can be used by state and local governments for a variety of public safety use cases, including:

- Any necessary expenses related to medical or public health needs incurred because of and during the pandemic.
- Pandemic Response: Expenses for public safety measures enacted in response to COVID-19.
- Payroll: Payroll expenses for public safety employees whose roles are largely dedicated COVID-19 response and mitigation efforts.
- Technology expenses incurred by local authorities and other entities related to COVID-19 response and mitigation efforts.

Department of Justice Coronavirus Emergency Supplemental Funding Program (CESF) Grant recipients can use the funds to cover the costs of personal protective equipment (PPE), to hire personnel, pay overtime costs, provide medical care to inmates and offset the costs of distributing more resources to areas hard-hit by COVID-19. Recipients of these grants have two years from January 2020 to use the funds.

(Source: Center for Digital Government)

Webinar: Community response and drone technology to improve outcomes from rural and remote cardiac arrest - The future is here!

The emergency medical community knows that timing is critical to improving survival outcomes for out-of-hospital cardiac arrest (OHCA) emergencies. Even when EMS arrives quickly, every minute delay results in reduced survival rates.

While it has been shown that bystander interventions can improve survival from Out of Hospital Cardiac Arrest (OHCA), rates of bystander cardio-pulmonary resuscitation (CPR) and automated external defibrillator (AED) usage remain low in many communities. One shortcoming with simply increasing the number of public AEDs is that three quarters of cardiac arrests occur in private locations where public access AEDs are unavailable.

To reach the OHCA patients that these public access defibrillation programs cannot reach, one novel strategy is utilizing the concept of "private access defibrillation," targeting community responders and drone technology, in order to improve access to AEDs and "time to first shock" in rural and remote communities as well as private locations.

If you are interested in learning more about how a program like this could work, you can participate in the upcoming webinar, Community Response and Drone Technology to Improve Outcomes from Rural and Remote Cardiac Arrest: The future is here!, on **Friday, April 23, 2021, at noon CST**.

This talk was given earlier this year at the 2021 National Association of EMS Physicians (NAEMSP) Annual Meeting, and was featured in the "NAEMSP Annual Conference Special" episode of the Prehospital Emergency Care podcast. You can listen to a "sneak peek" into the talk on the podcast's webpage for this episode.

To register for this webinar, visit the registration page.

For additional background information on this topic, you can read the study published by the authors of this talk in the Journal of the American Heart Association, or the United States Fire Administration's article reviewing the research on drone-delivered AEDs in rural settings.

(Source: ImageTrend)

Cyber Information and Incident Assistance Links

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

IdentityTheft.gov

IC3

Cybercrime Support Network

Apply Microsoft April 2021 security update to mitigate newly disclosed Microsoft Exchange vulnerabilities

Microsoft's April 2021 Security Update mitigates significant vulnerabilities affecting on-premises Exchange Server 2013, 2016, and 2019. An attacker could exploit these vulnerabilities to gain access and maintain persistence on the target host. The Cybersecurity and Infrastructure Protection Agency (CISA) strongly urges organizations to apply Microsoft's April 2021 Security Update to mitigate against these newly disclosed vulnerabilities. Note: the Microsoft security updates released in March 2021 do not remediate against these vulnerabilities.

Although CISA Emergency Directives only apply to Federal Civilian Executive Branch agencies, CISA strongly encourages state and local governments, critical infrastructure entities, and other private sector organizations to review ED 21-02 Supplemental Direction V2 and apply the security updates immediately.

For more information on required actions for federal agencies, and recommended actions for state, local, tribal and territorial government and private sector entities, read CISA's full current

General Information Links

[FTC scam list](#)

[CISA alerts](#)

[Law Enforcement Cyber Center](#)

[TLP Information](#)

government and private sector entities, read CISA's full current activity report.

(Source: CISA)

Using Aviary to analyze post-compromise threat activity in M365 environments

Aviary is a new dashboard that CISA and partners developed to help visualize and analyze outputs from its Sparrow detection tool released in December 2020. Sparrow helps network defenders detect possible compromised accounts and applications in Azure/Microsoft O365 environments. CISA created Sparrow to support hunts for threat activity following the SolarWinds compromise. Aviary—a Splunk-based dashboard—facilitates analysis of Sparrow data outputs.

CISA encourages network defenders wishing to use Aviary to facilitate their analysis of output from Sparrow to review CISA Alert: AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. **Note:** CISA has updated the Sparrow tool section of AA21-008A with instructions on using the Aviary tool.

(Source: CISA)

FBI and CISA issue joint alert on Mamba ransomware

The Federal Bureau of Investigations (FBI) recently issued a joint alert with the Department of Homeland Security/Cybersecurity Infrastructure and Security Agency (CISA) that "Mamba ransomware has been deployed against local governments, public transportation agencies, legal services, technology services, industrial, commercial, manufacturing, and construction businesses."

According to the Alert, the hacking group behind the Mamba ransomware attacks is weaponizing an open source tool used for disc encryption—DiskCryptor—to encrypt entire operating systems of victims. Once the operating system has been encrypted, a ransom note appears and demands payment for the decryption key.

The Alert lists the key artifacts, which can be accessed here.

(Source: Data Privacy and Security Insider)

Cost of a Cyber Incident: Systematic Review and Cross-Validation

In order to support stakeholders with understanding the impacts, costs, and losses from cyber incidents, CISA has cleared for release this October 2020 study, Cost of a Cyber Incident: Systematic Review and Cross-Validation. The objectives of the study are to enable cyber risk analysis, understand the benefits of cybersecurity investments, and inform cybersecurity resource allocation decisions. To achieve these objectives CISA's study reviews cost and loss estimates for a wide range of incidents. While the data analyzed in CISA's Cost Study can inform the order of magnitude of the potential costs associated with more recent events such as the SolarWinds compromise and Microsoft Exchange server exploit, the impacts associated with these events are not included in the study.

(Source: CISA)

Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities

On April 13, 2021, the Justice Department announced a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level e-mail service.

Through January and February 2021, certain hacking groups exploited zero-day vulnerabilities in Microsoft Exchange Server software to access e-mail accounts and place web shells (which are pieces of code or scripts that enable remote administration) for continued access.

Other hacking groups followed suit starting in early March after the vulnerability and patch were publicized. Although many infected system owners successfully removed the web shells from thousands of computers, others appeared unable to do so, and hundreds of such web shells persisted unmitigated. Today's operation removed one early hacking group's remaining web shells, which could have been used to maintain and escalate persistent, unauthorized access to U.S. networks. The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell (identified by its unique file path). This is unrelated to Microsoft's April 13 announcement.

(Source: DOJ)

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

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.

Section 504 Notice:
Section 504 of the Rehabilitation Act requires that FEMA grantees provide access to information for people with disabilities. If you need assistance accessing information or have any concerns about access, please contact FEMAWebTeam@fema.dhs.gov.

Subscribe to updates from EMR-ISAC

Email Address | Subscribe

Share Bulletin

Powered by

GOVDELIVERY

Privacy Policy | Cookie Statement | Help