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

The InfoGram

Volume 20 — Issue 20 | May 14, 2020

May is Wildfire Awareness Month

Wildfire season is already on us. Parts of Florida have mandatory evacuation zones in effect due to wildfire activity, and another blaze in Utah has been deemed an act of arson.

May is Wildfire Awareness Month and on top of all the usual wildfire-related threats to life and property, this year we have another facet to the wildfire response problem: a pandemic. Federal and state authorities are already drafting plans to manage spread in fire camps used by firefighters. See the Department of the Interior webpage on this topic for guidance on hiring firefighters and protecting them from COVID-19 during wildfire response.

In addition, if your agency is creating a COVID-19 response plan for managing personnel during this year's wildfire season, Wildfire Lessons Learned offers several recent postings on this topic from agencies around the country. You can also submit your own lessons learned to the site.

The U.S Fire Administration (USFA) maintains a wealth of information on wildfire response and wildland urban interface concerns. See the USFA website for things property owners can do to minimize the risk to homes and businesses against losses. You and your department can help homeowners with this process through continued outreach.

(Source: USFA)

COVID-19 Disinformation Activity: we're stronger together

Disinformation campaigns began almost immediately after COVID-19 became a global concern. Individuals, groups and even foreign governments are spreading false information about all aspects of the pandemic. In some cases, this information has prompted violence, attacks and sabotage.

We all recognize the situation is fluid and new details related to COVID-19's symptoms, transmission and vaccine research emerge almost daily. However, there is a difference between new information based on reliable research and misinformation intended to do harm.

The Cybersecurity and Infrastructure Security Agency (CISA) produced a one-page overview of this problem and how to ensure the information you and the public received is accurate, safe and reliable. COVID-19 Disinformation Activity addresses virus origin, scale, 5G technology, government response, prevention and treatment.

It also covers how to protect yourself from falling for misinformation and how to avoid spreading rumors. For example, pay attention to how something was written and to the source of the information. If what you are reading has language that sensationalizes the topic, seems to promote an agenda or triggers your emotions, someone probably wrote it that way to do exactly that: trigger you. This goes for any topic, not just pandemic response.

Societies facing a crisis respond better when united. People or groups wanting to

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

undermine that will work your fears to their advantage. Strongly consider the source and the wording of anything you read online before believing it or acting on it.

(Source: CISA)

FEMA releases National Response Framework and NIMS courses

The Federal Emergency Management Agency (FEMA) released two independent study course revisions this week.

National Response Framework, An Introduction (IS-800.d) is designed to provide guidance for the whole community. Within this broad audience, the National Response Framework (NRF) focuses on those who are involved in delivering and applying the response core capabilities. First responders and emergency managers are part of this audience.

This course revision incorporates the October 2019 NRF updates, including Community Lifelines. The Instructor Led Training (ILT) and classroom materials will be available later this year.

National Incident Management System (NIMS) Resource Management (IS-703.b) is designed to introduce federal, state, local, tribal and territorial emergency managers, first responders and incident commanders from all emergency management disciplines to NIMS Resource Management, as well as private industry and volunteer agency personnel responsible for coordination activities during a disaster.

This revision incorporates the October 2017 NIMS updates. The course is complete with the ILT and classroom materials.

See the National Preparedness Course Catalog for more information and additional courses.

(Source: FEMA)

Friday Webinars: Alternative Care Site security, funding sources

As part of the response to the pandemic, a number entities are involved in establishing ACS to expand capacity to combat COVID-19. These sites are often placed in non-traditional settings such as major convention centers. This presents many security challenges.

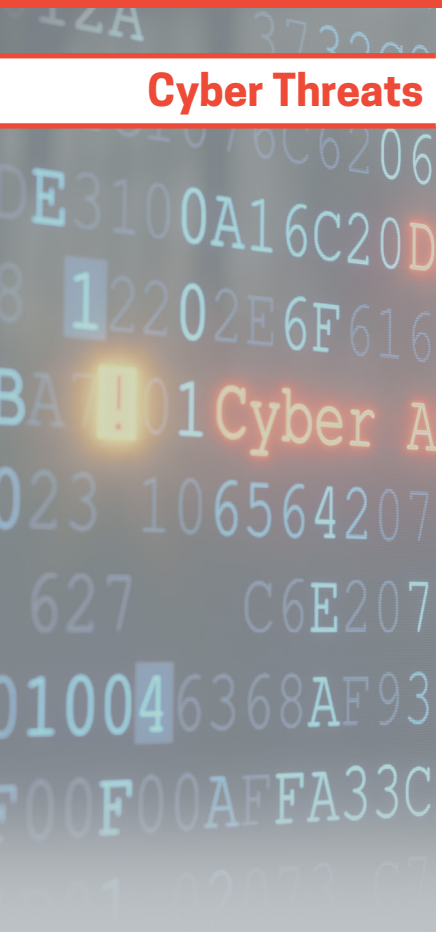
Join the upcoming Weekly Webinar Series- Securing the Health Sector this Friday, May 15, 2020, at 1 p.m. Eastern to learn about Securing Alternative Care Sites (ACS). This webinar series is sponsored by InfraGardNCR, the Department of Homeland Security and the Department of Health and Human Services (HHS); registration is required.

Also this Friday, government and private sector subject matter experts will provide information to health care planners about the physical security considerations for ACS, the planning required and the services available to assist the them.

On Friday, May 22, 2020, from 2:30-3:45 p.m. Eastern, HHS and FEMA are hosting the webinar Funding Sources for the Establishment and Operationalization of Alternate Care Sites. This webinar will feature an overview of this issue and discuss the ACS Funding Summary Tip Sheet.

(Source: Various)

Cyber Threats



Nearly 2,000 malicious COVIC-19-themed domains created every day

A new report from researchers found that more than 86,600 domains of the 1.2 million newly registered domain (NRDs) names containing keywords related to the COVID-19 pandemic from March 9, 2020 to April 26, 2020 are classified as "risky" or "malicious."

A study analyzing all new domain names containing keywords related to the COVID-19 pandemic found that the United States, Germany, Russia and Italy had the highest number of malicious coronavirus domains. The United States had far and away the most, with more than 29,000.

(Source: TechRepublic)

Executive order prohibits purchase of foreign power grid equipment

The United States government appears to be concerned foreign adversaries could be trying to plant malicious or vulnerable equipment in the country's power grid. That is why the latest executive order prohibits the acquisition of bulk-power system electric equipment that is designed, developed, manufactured or supplied by an entity that is "controlled by, or subject to the jurisdiction or direction of a foreign adversary."

This applies to transactions that have been determined to pose a risk to the grid itself, to critical infrastructure or the economy, or to national security or the security and safety of people.

(Source: Securityweek)

Coronavirus-related cyberattacks sure 192K in one week

Over the past three weeks, a research firm found 192,000 coronavirus-related cyberattacks per week, a 30 percent surge compared with the previous weeks. These cyberattacks encompass malicious websites with the word "corona" or "covid" in the domain name, files with "corona" in their name, and files attached to coronavirus-related phishing emails.

(Source: TechRepublic)

Cybercriminals using reCAPTCHA walls in phishing attacks

New research revealed cyber-criminals are increasingly using official reCAPTCHA walls to disguise malicious content from email security systems and trick unsuspecting users.

reCAPTCHA walls are typically used to verify human users before allowing access to web content, thus sophisticated scammers are beginning to use the Google-owned service to prevent automated URL analysis systems from accessing the actual content of phishing pages and to make phishing sites more believable in the eyes of the victim.

(Source: Infosec Magazine)

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.