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

The InfoGram

Volume 20 — Issue 34 | August 20, 2020

National Preparedness Month reminds us "Disasters Don't Wait"

September is National Preparedness Month and the theme for this year is "Disasters Don't Wait. Make Your Plan Today."

All disaster plans this year are affected and changed due to the pandemic's social distancing requirements, the need for masks and other PPE, and the need to quarantine people if they are exposed to COVID-19.

Each week in September, National Preparedness Month focuses on a different aspect of planning for disasters in your region. There are many resources available toward this goal on the Ready.gov website including directions for making a plan, information on special needs groups, how to build a kit and how to get involved in your community's preparedness activities.

The Ready.gov website has social media content for public relations campaigns already written as well as lists of applicable web resources, videos, graphics and logos to better engage with your audience. You can also access Ready.gov's informational pages on specific disasters to better target your messaging to preparing for disasters common in your area.

(Source: FEMA)

Study shows how hurricane evacuees may spread COVID-19

A recent study looks at how hurricane evacuees may spread COVID-19 and suggests a way to mitigate the problem.

Researchers with Columbia University and the Union of Concerned Scientists built a hurricane evacuation scenario in which 2.3 million residents of four Florida counties fled a Category 3 hurricane. They estimated where evacuees would flee using evacuation data from Hurricane Irma and matched it with a county-scale model of COVID-19 transmissions to determine how many cases would result from the evacuation and where they would occur.

The study assumed that COVID-19 transmission rates in destination counties increased during the evacuation period not at all or by 10 percent or 20 percent, representing the levels of public health directives put in place in destination counties and how well they were followed, as well as whether evacuees stayed with friends or family members or in hotels or shelters.

Researchers estimate that under the worst-case scenario, if people followed historic evacuation patterns and virus transmission rates increased by 20 percent in their destination counties, there would be roughly 61,000 additional COVID-19 cases in the origin and destination counties combined.

However, under the best-case scenario, if people instead evacuated to communities with low COVID-19 transmission rates and transmission rates did not increase in the destination counties, there could be as few as 9,100 additional cases resulting from the evacuation.

Researchers suggest mitigating potential increases linked to hurricane evacuation by directing people to counties with low COVID-19 transmission rates and making

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

sheltering options available that maintain social distancing guidelines.

(Source: Columbia University)

FDNY Safety Week 2020 videos available free through end of August

There is still time left to use the on-demand Fire Department of New York (FDNY) Safety Week 2020 video training. The online training is available free courtesy of the National Fallen Firefighter's Foundation and FDNY Foundation through August 31, 2020.

FDNY is sharing internal Safety Week training and information for the first time ever. The 2020 theme is "Get to Know Your Gear," which focuses on the personal protective equipment (PPE) the department uses day in and day out. This year, there could not be a more pertinent theme than maintaining protective measures for each member's personal safety, as well as for the people they interact with.

Registration is required, but current subscribers can view this content without registering.

(Source: FDNY Pro)

Building Resilient Infrastructure and Communities grant program

The Federal Emergency Management Agency (FEMA) announced the Notice of Funding Opportunity for the new Building Resilience Infrastructures and Communities (BRIC) grant program earlier this month. BRIC replaces the existing Pre-Disaster Mitigation program. The BRIC priorities are to incentivize:

- Public infrastructure projects.
- Projects that mitigate risk to one or more lifelines.
- Projects incorporating nature-based solutions.
- The adoptions and enforcement of modern building codes.

States, local communities, tribes and territories can apply for BRIC grants between September 30, 2020 and January 29, 2021. FEMA has $500 million allotted for pre-disaster mitigation activities through BRIC grants.

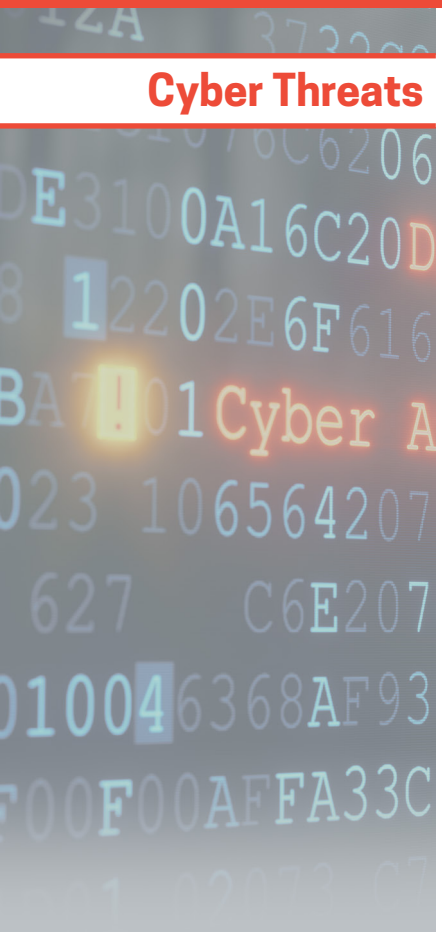
A key requirement for eligibility is that mitigation projects must, at a minimum, be in conformance with the latest published editions (meaning either of the two most recently published editions) of relevant consensus-based codes, specifications and standards incorporating the latest hazard-resistant designs.

In August and September, FEMA will host a series of overview webinars on BRIC and two webinars on "Avoiding Application Pitfalls." Registration is required for all upcoming webinars.

This new grant program stems from Disaster Recovery Reform Act of 2018 legislation. Reforms from this legislation originated as lessons learned from the economic disruption and increased nationwide disaster costs caused by the historic 2017 hurricanes and wildfires. See the details about BRIC at Grants.gov.

(Source: FEMA)

Cyber Threats



Cyber Essentials Toolkit: Your Systems, What Makes You Operational

The Cybersecurity and Infrastructure Security Agency (CISA) just released Chapter 3 of its Cyber Essentials Toolkit: Your Systems, What Makes You Operational.

This chapter emphasizes protecting the information and applications on your network. Organizations that build security into and around critical assets and applications strengthen their technical cyber hygiene. This Cyber Essentials Toolkit recommends actionable steps leaders can take to manage network assets with the goal of protecting information and securing hardware and software.

The Cyber Essentials Toolkit is for small companies and local government agencies. The toolkit is a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for information technology professionals and leadership to work toward full implementation of each Cyber Essential. Previous chapters focus on cybersecurity as it relates to leadership and users.

Each chapter focuses on recommended actions to build cyber readiness into the six interrelated aspects of an organizational culture of cyber readiness. In future months, you will see toolkits that focus on organizational tools, plans, processes, and other tips to make organizational cybersecurity easy and seamless.

(Source: CISA)

ReVoLTE attack allows hackers to listen in on mobile calls

Researchers discovered an attack on Voice over LTE (VoLTE) mobile communications protocol that can break its encryption and allow attackers to listen in on phone calls.

Dubbed ReVoLTE, the attack exploits an implementation flaw in the LTE cellular protocol that exists at the level of a mobile base station. ReVoLTE makes use of a predictable keystream reuse, an encryption scenario in which stream ciphers, or encryption keys, are vulnerable to attack if the same key is used in a predictable fashion. This can allow threat actors to recover contents of an encrypted VoLTE call.

The attack is novel in that standard cellular protocols typically aren't targeted for hacking because researchers "never have the energy to deal with" the legwork involved of untangling the pages of documentation about the standard itself.

(Source: Threat Post)

Dutch hackers found a simple way to mess with traffic lights

Hijacking traffic lights over the internet looks easy in the movies, but real-world traffic-light hacking, demonstrated by security researchers in years past, has proven tougher, requiring someone to be within radio range of every target light.

Dutch security researchers will present findings about vulnerabilities in an "intelligent transport" system that would allow them to influence traffic lights in at least 10 different cities in the Netherlands over the internet. Their hack would spoof nonexistent bicycles approaching an intersection, tricking the traffic system into giving those bicycles a green light and showing a red light to any other vehicles trying to cross in a perpendicular direction.

(Source: Wired)

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.