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

# The InfoGram

Volume 21 — Issue 26 | July 1, 2021

## New guidance from CDC on post-COVID conditions

As new data continues to emerge on the COVID-19 pandemic, clinicians and scientists have become increasingly alarmed with a syndrome that has been informally termed "long COVID" – continued symptoms of COVID-19 that last 3 weeks or more after the diagnosis. Long COVID patients have a broad range of overlapping and often debilitating symptoms, such as muscle pain or chest pain, difficulty breathing or shortness of breath, and severe fatigue. The physical symptoms of long COVID seem to be independent of the severity of the initial infection symptoms, according to preliminary research on this emerging pattern of illness.

In June 2021, the Centers for Disease Control and Prevention (CDC) released Evaluating and Caring for Patients with Post-COVID Conditions: Interim Guidance. The CDC defines "post-COVID conditions" as "an umbrella term for the wide range of physical and mental health consequences experienced by some patients that are present four or more weeks after SARS-CoV-2 infection, including by patients who had initial mild or asymptomatic acute infection."

In addition to offering the most updated recommendations for health care providers, the CDC's new guidance provides resources for patients suffering with these conditions, including information on very recently established support and advocacy groups for long COVID patients.

An April 2021 article in FireRescue1 stresses that, for those who have recovered from or are recovering from COVID-19, it is important to watch for potential long-term symptoms and to allow adequate time for the body to recover. The fire service will need to be attentive to the ability of firefighters to respond to full operational capacity following a prolonged recovery period.

Knowledge of post-COVID conditions is likely to change rapidly with ongoing research. The CDC recommends that both healthcare professionals and patients continue to check CDC's website for updates on evolving guidance for post-COVID conditions.

*(Sources: CDC, FireRescue1)*

## FEMA seeks public feedback on two Urban Search & Rescue resource types

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

Subscribe here

The recent tragic building collapse of the Surfside condo tower in Miami-Dade County, Florida resulted in deployment of several urban search and rescue teams around the country to help with rescue and recovery efforts. These elite resources are highly technically skilled and technologically equipped, and their capabilities are mission-critical during a major disaster such as the Surfside condo structural collapse.

The Federal Emergency Management Agency's (FEMA's) National Integration Center is seeking public feedback on two Urban Search and Rescue (US&R) Job Title/Position Qualifications. These resource typing documents enhance the interoperability and effectiveness of mutual aid by establishing baseline qualifications for Urban Search & Rescue Logistics and Medical Specialists. This facilitates the sharing of deployable US&R resources at all jurisdictional levels.

National engagement provides an opportunity for interested parties to comment on the draft documents to ensure they are relevant to all implementing partners. If you have experience with urban search and rescue, you can help by giving FEMA your feedback on these two resource-typed positions.

This 30-day national engagement period will conclude at **5:00 p.m. EST on July 29, 2021.** To provide feedback, review the draft documents, complete the feedback form [Excel file download, 16 KB] with your comments, and submit the form to FEMA-NIMS@fema.dhs.gov no later than 5:00 p.m. EST on July 29, 2021.

*(Source: FEMA)*

## Updated Funding Mechanisms Guide for Public Safety Communications from CISA, SAFECOM, NCSWIC

For public safety personnel to effectively respond to incidents and events, there must be reliable, secure, operable, and interoperable communications systems in place. However, the rapid rate of technology evolution means public safety agencies must also plan for the ongoing integration and alignment of technologies such as Land Mobile Radio (LMR), Next Generation 911 (NG911), FirstNet Authority's Nationwide Public Safety Broadband Network, as well as alerts, warnings, and notifications systems.

In their efforts to ensure emergency communication systems are in a secure and interoperable state, the public safety community will likely continue to face funding challenges.

Public safety agencies need to be able to balance integration and alignment of communications technologies with other competing priorities and funding needs. They also need to be able to prepare clear and concise budget options that identify multiple revenue streams, especially given fluctuating funding levels.

To address these needs, the Cybersecurity and Infrastructure Security Agency (CISA), in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), recently released an updated Funding Mechanisms Guide for Public Safety Communications to assist public safety agencies in identifying funding sources for emergency communications projects. This update builds on the 2015 version of the Guide. It highlights strengths, challenges, and opportunities for public safety communications funding, and incorporates examples of real-world successes and challenges from states and localities.

The Funding Mechanisms Guide assists agencies in determining whether a particular strategy for obtaining funding is suitable for their community. To assist in identifying appropriate solutions, this document summarizes the Emergency Communications System Lifecycle Planning Guide Compendium's pre-planning steps. These steps help agencies look past initial capital investments to consider acquisitions, repairs, and upgrades as necessary costs, and plan for the entire system lifecycle. Along with this guidance, the document includes an extensive inventory of all different types of funding mechanisms, and a list of resources for additional considerations, guidance, and best practices.

The Funding Mechanisms Guide, along with many of the resources referenced within the Guide, are available within CISA's Sustaining Public Safety Communications Systems Documents collection.

CISA encourages public safety agency leaders to visit SAFECOM's Funding Resources page, where you can find guidance on grant funding for emergency communications projects, as well as brief descriptions of all of the resources provided in CISA's Sustaining Public Safety Communications Systems Documents collection.

*(Source: CISA)*

## Webinar: Emergency Response at the January 6 Incident at the US Capitol

The January 6 incident at the United States Capitol presented a unique set of circumstances for the District of Columbia (DC) Fire and EMS Department: a planned protest turned into a riot. There are important lessons to be learned about unified command; working with multiple agencies; having adequate resources; and making decisions in a changing tactical environment.

The International Association of Fire Chiefs (IAFC) will host a webinar on **Tuesday, July 20, 2021, from 1:00 to 2:00 p.m. EST** to discuss the emergency response at the January 6 Incident at the U.S. Capitol. At this webinar, the Chief and Deputy Chief from the DC Fire and EMS Department will discuss the issues that arose on January 6 and lessons that can be learned for fire and EMS agencies.

This webinar is free to join and open to anyone, but registration is required.

*(Source: IAFC)*


## Cyber Information and Incident Assistance Links

## CISA's CSET Tool sets sights on ransomware threat

The Cybersecurity and Infrastructure Security Agency (CISA) has released a new module in its Cyber Security Evaluation Tool (CSET): the Ransomware Readiness Assessment (RRA). CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET—applicable to both information technology (IT) and industrial control system (ICS) networks—enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations.

CISA strongly encourages all organizations to take the CSET Ransomware Readiness Assessment, available at https://github.com/cisagov/cset/releases/tag/v10.3.0.0.

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

*(Source: CISA)*

## CISA is developing a catalog of Bad Practices

As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated Critical Infrastructure or National Critical Functions (NCF) should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk in a manner commensurate with the criticality of those NCFs to national security, national economic security, and/or national public health and safety.

CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public.

Entries in the catalog will be listed here as they are added.

*(Source: CISA)*

## Microsoft: SolarWinds hackers continue to target IT companies

Microsoft says it has observed new activity associated with Nobelium, the Russia-linked threat actor that compromised IT management and monitoring solutions provider SolarWinds.

The SolarWinds attack was brought to light in early December 2020 and it involved compromising SolarWinds' Orion monitoring product to deliver trojanized updates to the company's customers worldwide, in an effort to breach their networks.

On Friday, Microsoft revealed that it recently observed password spray and brute-force attacks associated with current Nobelium activity, with targets identified in 36 countries.

*(Source: Security Week)*

## BIOS Disconnect: new high-severity bugs affect 128 Dell PC and tablet models

Cybersecurity researchers on Thursday disclosed a chain of vulnerabilities affecting the BIOSConnect feature within Dell Client BIOS that could be abused by a privileged network adversary to gain arbitrary code execution at the BIOS/UEFI level of the affected device.

In all, the flaws affect 128 Dell models spanning across consumer and business laptops, desktops, and tablets, totaling an estimated 30 million individual devices. Worse, the weaknesses also impact computers that have Secure Boot

enabled, a security feature designed to prevent rootkits from being installed at boot time in memory.

CISA's National Cyber Awareness System encourages users and administrators to review the Dell Security Advisory DSA-2019-084 and apply the necessary update.

*(Source: The Hacker News)*

## NSA shares guidance on securing voice, video communications

The National Security Agency (NSA) has shared mitigations and best practices that systems administrators should follow when securing Unified Communications (UC) and Voice and Video over IP (VVoIP) call-processing systems.

Since these communication systems are tightly integrated with other IT equipment within enterprise networks, they also inadvertently increase the attack surface by introducing new vulnerabilities and the potential for covert access to an organization's communications. Improperly secured UC/VVoIP devices are exposed to the same security risks and targeted by threat actors through spyware, viruses, software vulnerabilities, and other malicious means if not adequately secured and configured.

Visit the NSA's website to read the abridged and full versions of NSA's guidance.

*(Source: Bleeping Computer)*

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