U.S. Fire Administration | FEMA

**Subscribe to updates from EMR-ISAC**

Email Address e.g. name@example.com

Subscribe

# EMR-ISAC InfoGram Sept. 23 - Suicide Prevention Awareness Month; NIST requests input on cybersecurity guidance for telemedicine

**Share Bulletin**

EMR-ISAC sent this bulletin at 09/23/2021 03:08 PM EDT

View as a webpage / Share

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

## The InfoGram

Volume 21 — Issue 38 | September 23, 2021

## September is Suicide Prevention Awareness Month

September is Suicide Prevention Awareness Month, a time set aside for building awareness around this very real and concerning problem among emergency responders and to learn more about what you can do to help a colleague who may be struggling.

In the past few years more first responders have died by suicide than in the line of duty. The Department of Justice's Office of Community Oriented Policing (COPS Office) released a report to the United States Congress in April 2021 in response to an increase in suicides among law enforcement officers and other first responders. After evaluating behavioral health programs across the nation, the COPS Office report found that departments have been most successful in lowering their suicide rates by creating support networks such as peer-to-peer programs and lowering the stigma and fear associated with asking for help.

There are many resources and support networks available to the first responder community to help in suicide prevention efforts. This article highlights a few prominent programs.

- The National Fallen Firefighter Foundation's (NFFF's) Everyone Goes Home program provides a 2-page guide on what to do immediately, in the short term, and in the long term if you are concerned someone may be thinking about suicide.
- The Firefighter Behavioral Health Alliance (FBHA) provides behavioral health workshops to fire departments, EMS and dispatch organizations across the globe, focusing on behavioral health awareness, with a strong emphasis towards suicide prevention.
- The International Association of Chiefs of Police's (IACP's) National Consortium on Preventing Law Enforcement Suicide provides a suicide prevention toolkit and many other resources.
- The COPS Office provides resources, guidance and funding with its Law Enforcement Mental Health and Wellness Programs.
- The Code Green Campaign is a first responder-oriented mental health advocacy and education organization.
- The Centers for Disease Control and Prevention (CDC) provides resources for suicide prevention among the healthcare workforce.

Finally, there are several crisis hotlines available. It is a good idea to have this information posted in prominent locations within your organization:

- The National Suicide Prevention Lifeline: 1-800-273-TALK (8255).
- The National Volunteer Fire Council's Fire/EMS Helpline: 1-888-731-FIRE (3473).
- COPLINE, a not-for-profit organization provides a confidential 24/7 hotline supporting current and retired law enforcement and their families: 1-800- COP-LINE (1-800-267-5463).
- Safe Call Now, a confidential, comprehensive, 24-hour crisis line and support service for first responders, emergency services personnel, medical professionals and their family members nationwide: 1-206-459-3020.
- Suicide.org lists individual state helplines.

*(Sources: Various)*

## NIST requests comments on draft guidance for cybersecurity within telemedicine by Oct. 4

### 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

Although it was the COVID-19 pandemic that accelerated the adoption of telemedicine by emergency medical services (EMS) and 911 systems across the country, its use is likely only going to continue to grow. According to the American Ambulance Association, telemedicine will be a key tool to help communities achieve the vision of a people-centered EMS system described by EMS Agenda 2050.

Often, transportation is a barrier to receiving healthcare, which means EMS becomes that transportation even when the medical problem itself is non-urgent. Telemedicine can be used to triage patients, decreasing non-emergent ambulance transports, or to enable a higher level of care when access or distance prevent physical assessment.

Telemedicine uses technology to connect patients to healthcare practitioners remotely. Telehealth technology has advanced alongside the "Internet of Things (IoT)", which brings novel capabilities to consumers in their homes. However, along with those capabilities come cybersecurity risks and concerns around how the home environment is secured against breaches or cyberattacks.

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) has released a new draft project description for Mitigating Cybersecurity Risk in Telehealth Smart Home Integration. This project will result in a practice guide that describes a reference architecture for smart home integration with healthcare systems as part of a telehealth program.

EMS agencies interested in starting a telehealth program or who have already started one may want to review this project description and submit comments online **on or before October 4, 2021**. You can also help shape and contribute to this project by joining the NCCoE's Healthcare Community of Interest. If you would like to take part in this community, send an email to hit_nccoe@nist.gov detailing your interest.

*(Source: NIST NCCoE)*

---

## National Fire Prevention Week is Oct. 3-9

If you or someone in your department is a fire and life safety educator or fire prevention officer, now is a great time to do some planning for National Fire Prevention Week, which will take place **October 3-9**. The National Fire Protection Association (NFPA) has partnered with the United States Fire Administration (USFA) to promote this campaign with fire departments, community educators, and the public.

The theme of this year's Fire Prevention Week is "Learn the Sounds of Fire Safety," focusing on educating the public on the different sounds smoke and carbon monoxide (CO) alarms make.

The NFPA has developed new resources for this year's campaign on its dedicated website for Fire Prevention Week. Here are just a few:

- The 2021 campaign video is featured on the "About" page, highlighting the sounds of different alarms, and what to do when hearing these sounds. This video incorporates narration in American Sign Language. The NFPA has also created a video for children on its Sparky.org website.
- A Safety Tip Sheet, Learn the Sounds of Fire Safety, highlighting both smoke alarms and CO alarms. A version is also available for those who are deaf or hard of hearing.
- The 2020 edition of the Educational Messages Desk Reference (EMAC) is now available, with new sections for pet fire safety and youth firesetters. This resource will help to ensure your outreach materials have accurate messaging appropriate to your audiences.

The USFA provides many valuable resources for public education and outreach that can support this year's Fire Prevention Week. The USFA's Fire Prevention and Safety Pictographs collection includes pictographs for carbon monoxide and smoke alarms, to help you reach everyone in your community, especially those with different cultural backgrounds, low English proficiency, or low literacy levels. You can explore the USFA's Fire Prevention and Public Education web pages for many more free resources.

The weeks leading up to Fire Prevention Week are a great time to reach out to your local media with a press release from your organization recognizing Fire Prevention Week, containing safety messages for your community. Templates for press releases and guidance for working with the media are available from the NFPA and the USFA.

The NFPA and USFA encourage you to use social media to promote this year's Fire Prevention Week with your own campaigns, and by using the hashtag **#FirePreventionWeek**. The NFPA provides many social media resources to support this year's theme in the "Toolkit" section of its website, and the USFA has a large collection of resources to support social media campaigns about fire safety.

*(Sources: NFPA, USFA)*

---

## DHS S&T and FEMA partner on "New Phase of Emergency Alerting" webinar series, first webinar on Oct. 7

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T), in partnership with the Federal Emergency Management Agency (FEMA), will host a new quarterly webinar series on "the new phase of emergency alerting." The first webinar in this series will explain FEMA's Integrated Public Alert and Warning System (IPAWS) and the IPAWS Program Planning Toolkit.

This first webinar in the quarterly series, "What is the FEMA IPAWS Program Planning Toolkit?", is scheduled for **October 7, from 1:00 to 2:15 p.m. EST**. Attendees will leave this webinar with an understanding of how the Toolkit can help them distribute authenticated life-saving information to the public, including Wireless Electronic Alerts to cell phones. The webinar is open to everyone but registration is required.

See DHS S&T's New Phase of Emergency Alerting webinar series page for future webinar information and dates.

*(Source: DHS S&T)*

**Cyber Threats**


## 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

## CISA, FBI, and NSA release Conti ransomware advisory to help organizations reduce risk of attack

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) published a cybersecurity advisory on September 22 regarding increased Conti ransomware cyberattacks. The advisory includes technical details on the threat and mitigation steps that public and private sector organizations can take to reduce their risk to this ransomware.

The advisory can be found here and is available on the new, whole-of-government ransomware website, StopRansomware.gov.

*(Source: CISA)*

## Treasury takes robust actions to counter ransomware

As part of the whole-of-government effort to counter ransomware, the U.S. Department of the Treasury on September 21 announced a set of actions focused on disrupting criminal networks and virtual currency exchanges responsible for laundering ransoms, encouraging improved cyber security across the private sector, and increasing incident and ransomware payment reporting to U.S. government agencies, including both Treasury and law enforcement.

The Department of the Treasury's actions include its Office of Foreign Assets Control's (OFAC) designation of SUEX OTC, S.R.O. (SUEX), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors. SUEX has facilitated transactions involving illicit proceeds from at least eight ransomware variants.

OFAC also released an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The Advisory emphasizes that the U.S. government continues to strongly discourage the payment of cyber ransom or extortion demands and recognizes the importance of cyber hygiene in preventing or mitigating such attacks.

*(Source: U.S. Department of the Treasury)*

## CISA releases two ICT supply chain resources to improve information sharing and assist small and medium-sized businesses

The increase in digitization and use of information and communications technology (ICT) has improved the ability of many companies to provide National Critical Functions. At the same time, nation-states seeking to cause harm to the United States (i.e., espionage or stealing information) have thousands of companies and entry points to choose from.

The ICT Supply Chain Risk Management Task Force, a public-private partnership for enhancing supply chain resilience, has developed two new resources: 1) to address liability challenges on sharing supply chain threat information and, 2) to assist small and medium-sized businesses (SMBs) with mitigating ICT

small and medium-sized businesses (SMBS) with mitigating ICT supply chain risks. The first resource, Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information, offers subject matter expert research on legal and policy considerations for giving liability protection to the private sector in order to promote information sharing about suspect suppliers. The second resource, Operationalizing the Vendor SCRM Template for Small and Medium-sized Businesses, helps IT and communications small and medium-sized businesses assess their risk posture from the perspective of the acquirer, integrator, and supplier when procuring ICT hardware, software, and services or acquiring new contracts.

*(Source: CISA)*

## Researchers compile list of vulnerabilities abused by ransomware gangs

Security researchers are compiling an easy-to-follow list of vulnerabilities ransomware gangs and their affiliates are using as initial access to breach victims' networks. While these bugs have been or still are exploited by one ransomware group or another in past and ongoing attacks, the list has also been expanded to include actively exploited flaws. The list comes in the form of a diagram providing defenders with a starting point for shielding their network infrastructure from incoming ransomware attacks.

This year alone, ransomware groups and affiliates have added multiple exploits to their arsenal, targeting actively exploited vulnerabilities.

*(Source: Bleeping Computer)*

## DDoS attacks are becoming more prolific and more powerful, warn cybersecurity researchers

There's been a rise in distributed denial of service (DDoS) attacks in recent months in what cybersecurity researchers say is a record-breaking number of incidents. But it isn't just the rise in DDoS attacks that makes them disruptive; cyber criminals are adapting new techniques to evolve their attacks in order to help them bypass cloud-based and on-premise defenses. DDoS attacks have become more effective during the past year due to the added reliance on online services.

However, in the majority of cases it's possible to defend against DDoS attacks by implementing the industry's best current practices to maintain availability of services in the face of an incident. These practices include setting specific network access policies as well as regularly testing DDoS defenses to confirm they can protect the network from attacks.

*(Source: ZDNet)*

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