U.S. Fire Administration | FEMA

EMR-ISAC InfoGram May 12 – Civil unrest: resources for fire and EMS agencies; New mobile app brings counterterrorism intelligence to first responders

EMR-ISAC sent this bulletin at 05/12/2022 03:03 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 22 — Issue 19 | May 12, 2022

Civil unrest: preparedness and planning resources for fire and EMS agencies

The United States Supreme Court (SCOTUS) has been deliberating this year on several cases that could be highly contentious and result in significant protests and rallies across the country.

A higher frequency of protests and rally events are now occurring, due to a premature release of a SCOTUS draft ruling on one specific case, and these incidents are expected to continue in the coming months.

Extremist groups have historically exploited these otherwise celebrated First Amendment-protected assemblies with deliberate attempts to escalate peaceful protests into violence and destruction of property.

Individual acts of vandalism or arson may also occur more frequently in a climate of discontent, and fire is often used as a means of intimidation not only to destroy property, but also to inflict fear and injury.

Planning and preparedness are crucial for public safety agencies to successfully coordinate management and response during any large public gathering, but especially if these gatherings deteriorate into civil unrest. Close coordination with law enforcement as the lead agency is essential for response during civil unrest.

Highlights

The following are a selection of resources from the United States Fire Administration (USFA) and partner agencies to support fire and EMS safety, preparedness, planning, and response in environments of civil unrest. This list is not intended to be exhaustive:

- Civil Unrest Response Best Practices, a collection of resources for fire and EMS from the USFA, and associated reference aid from the National Highway Traffic Safety Administration's Office of EMS.
- A sample Civil Unrest Standard Operating Procedure, supporting the National Fallen Firefighters Foundation's Initiative 12: Violent Incident Response.
- The International Association of Firefighters' 2020 webinar recording, Caught in the Middle: Fire Department Response During Civil Unrest. This webinar recording is free, but registration is required for access.
- First Responder's Toolboxes on Protection Considerations for Violent Extremist Threats to Public Officials, Complex Operating Environment – Special and Other Significant Events, and many other Toolboxes from the National Counterterrorism Center (NCTC). The entire collection, including those designated For Official Use Only (FOUO) are available on the Homeland Security Information Network, the Law Enforcement Enterprise Portal and the NCTC's newly launched aCTknowledge portal.
- The National Fire Protection Association's Standard on Fire Department Occupational Safety, Health, and Wellness Program (NFPA 1500) requires agencies that adopt this standard to plan and train for violent incidents.
- The National Tactical Officers Association's training for multiple response disciplines to respond together with law enforcement during mass casualty and other critical incidents.
- Fire as a Weapon Action Guide, from the Cybersecurity and Infrastructure Security Agency, within its Active Assailant Security resources collection.
- The Department of Justice's awareness training on First Amendment-protected activities.
- Lessons learned by law enforcement after the protests in many cities across the United States in 2020, and best practices and tactics for law enforcement response to First Amendment assemblies, from the Major Cities Chiefs Association.
- Lessons learned by hospitals after the George Floyd

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

protests in Minneapolis and technical assistance on protecting hospitals during civil unrest, from the Office of the Assistant Secretary for Preparedness and Response, Technical Resources, Assistance Center, and Information Exchange (ASPR TRACIE).

(Sources: Various)

New mobile app brings timely counterterrorism intelligence to first responders and homeland security professionals

The National Counterterrorism Center's (NCTC's) aCTknowledge is a first-of-its-kind mobile app and website that provides timely and unclassified counterterrorism reports and situational awareness notifications. It is available to all public servants who play a role in protecting their community.

Now available on the Apple App Store and on Google Play, this digital platform features a searchable library of unclassified counterterrorism reporting, analysis, and training resources, featuring breaking potential counterterrorism events, counterterrorism policies, and emergent terrorist tactics, techniques, and procedures. NCTC experts developed the app in partnership with law enforcement agencies as a way to deliver a one-stop shop for counterterrorism experts across the nation.

Additionally, NCTC's aCTknowledge offers reference guides to aid in rapid response and deployment, helping you protect your local community.

The NCTC was established at the recommendation of the 9/11 Commission and was given the responsibility for integrating whole-of-government analysis, strategic planning, and information sharing with state, local, tribal, territorial, and federal partners through the Intelligence Reform and Terrorism Prevention Act. NCTC has the unique authority to access both domestic and foreign terrorism information.

Today, NCTC produces analysis, maintains the authoritative database of known and suspected terrorists, shares information, and conducts strategic operational planning. The Center plays a vital role in protecting the Homeland and U.S. interests around the world from the threat of terrorism.

To learn more about aCTknowledge and to request access, visit the website and download the aCTknowledge 1-page fact sheet.

(Source: NCTC)

EMS Week honors emergency medical services professionals for Rising to the Challenge

The 47th annual EMS Week will be observed from May 15-21. This year's theme is "Rising to the Challenge."

The emergency medical services (EMS) have stood strong despite many challenges over the past year. The United States Fire Administration's (USFA's) COVID-19 Special Study has been tracking fire and EMS responses involving COVID-19 since January 2020. The data from 2021 show that fire and EMS responded to more than 300,000 calls where COVID-19 was suspected or confirmed. EMS professionals have had higher rates of occupational exposure to COVID-19, as frontline workers treating patients.

EMS has also endured a myriad of challenges made worse by the pandemic, including workforce shortages, supply shortages and more difficulty getting the training they need.

The USFA joins the National Association of Emergency Medical Technicians (NAEMT) and the American College of Emergency Physicians (ACEP), working to ensure that the important contributions of EMS providers in safeguarding the health, safety and well-being of their communities are fully celebrated and recognized.

Each day of EMS Week has its own theme:

- Sunday, May 15 - Health, Wellness and Resilience Day.
- Monday, May 16 - Education Day.
- Tuesday, May 17 - EMS Safety Day.
- Wednesday, May 18 - EMS for Children Day.
- Thursday, May 19 - Save-A-Life Day.
- Friday, May 20 - EMS Recognition Day.

EMS agencies are encouraged to plan activities and events around these themes in their communities. Traditionally, ACEP has provided printed planning guides for EMS Week, but this year, all content will be electronic and easily accessible on EMSWeek.org.

Visit EMSWeek.org for social media ads, images and video resources to help promote and celebrate EMS professionals during the week. You can also read inspiring stories about how EMS professionals are staying strong in these challenging times.

(Sources: EMSWeek.org, ACEP, NAEMT, USFA)

Webinar: FirstNet on communications in healthcare settings and special events

FirstNet Authority is hosting a webinar on **Thursday, May 26, 2-3 p.m. EST** as part of its FirstNet Emergency Management Webinar Series, entitled Extended Primary Users on FirstNet: You're not in it alone.

This webinar is an opportunity to learn about how FirstNet services can help FirstNet's extended primary users, who could be called upon to support first responders during an emergency or its aftermath, such as those who support essential government services, education, transportation, and utilities.

Speakers in this webinar will focus on the extended community supporting first responders for public safety telecommunications in healthcare settings and during special events.

Discussion will include:

- A vision of how FirstNet can be incorporated into a total hospital response environment in order to more effectively connect internal staff, external hospital resources as well as local and state responders.
- How extended primary partners can enable your event command and control operations to run seamlessly through logistical coordination, surveillance equipment (360-degree cameras, drones), and incident management software.

This webinar is intended for public safety and other government personnel and will be recorded

This webinar is intended for public safety and other government personnel and will be recorded. The recording may be distributed to attendees and other stakeholders upon request.

For more information and to register, visit FirstNet Authority's announcement for this webinar.

(Source: FirstNet Authority)

Cyber Incident Assistance

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

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information

StopRansomware.gov

CISA's Known Exploited Vulnerabilities Catalog

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

CISA: Alert (AA22-131A) - Protecting Against Cyber Threats to Managed Service Providers and their Customers

The cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA), (NSA), (FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue. This joint Cybersecurity Advisory (CSA) provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

(Source: CISA)

U.S. Government attributes cyberattacks on SATCOM networks to Russian state-sponsored malicious cyber actors

CISA and the Federal Bureau of Investigation (FBI) have updated the joint cybersecurity advisory, Strengthening Cybersecurity of SATCOM Network Providers and Customers, originally released March 17, 2022, with U.S. government attribution to Russian state-sponsored malicious cyber actors. The United States assesses Russia launched cyberattacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the Russia invasion, and those actions had spillover impacts into other European countries.

(Source: CISA)

NIST updates cybersecurity guidance for supply chain risk management

A new update to the National Institute of Standards and Technology's (NIST's) foundational cybersecurity supply chain risk management (C-SCRM) guidance aims to help organizations protect themselves as they acquire and use technology products and services. It forms part of NIST's response to Executive Order 14028: Improving the Nation's Cybersecurity, specifically Sections 4(c) and (d), which concern enhancing the security of the software supply chain.

Because cybersecurity risks can arise at any point in the life cycle or any link in the supply chain, the guidance now considers potential vulnerabilities such as the sources of code within a product, for example, or retailers that carry it. The publication offers help to the varied groups in its intended audience, which ranges from cybersecurity specialists and risk managers to systems engineers and procurement officials.

(Source: NIST)

Critical vulnerability exploited to 'destroy' BIG-IP appliances

CVE-2022-1388 is a critical remote code execution vulnerability that can easily be exploited by an unauthenticated attacker. Attacks can be launched from the internet against devices that expose their management interface — there are a few thousand such devices — or from the targeted organization’s network. Patches and mitigations were announced on May 4 and the first attack attempts were spotted within days.

The US Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added CVE-2022-1388 to its Known Exploited Vulnerabilities Catalog. Federal agencies are required to address the flaw by May 31, but hopefully they have already rolled out patches or mitigations given the elevated risk.

BIG-IP application delivery controllers are used by some of the world’s biggest organizations — F5 says 48 of Fortune 50 companies are customers.

(Source: Security Week)

Ransomware tracker: the latest figures [May 2022]

Although the number of reported ransomware attacks remained stable throughout April, cybersecurity experts noticed that one group in particular boosted its activity.

The Conti ransomware gang was linked to at least 50 incidents in April, including a devastating attack on Costa Rican government agencies. The attack prompted the country’s newly inaugurated president to declare a state of emergency, and the U.S. Department of State is offering a multimillion-dollar bounty for information that leads to the identification or arrest of Conti members.

But Conti wasn’t the only group launching attacks — ALPHV, Black Basta, LockBit 2.0, Cl0p, and others struck healthcare organizations, construction firms, government agencies, and a wide range of other organizations.

(Source: The Record)

Tenet says ‘cybersecurity incident’ disrupted hospital operations

Tenet, one of the largest for-profit health systems in the U.S., said it experienced a “cybersecurity incident” last week that disrupted some acute care operations. Most critical functions have been restored, while affected facilities are beginning to resume normal operations, according to a statement Tuesday from the Texas-based operator.

Tenet, which operates 60 hospitals and roughly 550 other care sites across 34 states, is the latest health system to be affected by a cybersecurity breach, which have been increasing in severity in the U.S. and in the healthcare industry.

(Source: Cybersecurity Dive)

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.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your Subscriber Preferences Page. You will need to use your e-mail address to log in. If you have questions or problems with the subscription service, please contact subscriberhelp.govdelivery.com.

Privacy Policy | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

Subscribe to updates from EMR-ISAC

Email Address e.g. name@example.com

Subscribe

Share Bulletin

Powered by

GOVDELIVERY

Privacy Policy | Cookie Statement | Help