U.S. Fire Administration | FEMA

EMR-ISAC InfoGram July 22 – Call for participants in COVID-19 study surveying first responders; Webinar on violent extremist recruitment tactics

EMR-ISAC sent this bulletin at 07/22/2021 03:58 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 21 — Issue 29 | July 22, 2021

Call for participants in study measuring impact of COVID-19 on first responder organizations

The University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) is calling for participants in an ongoing study to monitor and mitigate the impact of COVID-19 on public safety. If you are a member of a first responder organization (law enforcement, emergency medical services and/or fire department), and you were involved in your agency's response to COVID-19, please take a moment to fill out this short survey. It is estimated to take about six to eight minutes to complete. All responses will be anonymous and reported in ways that protect your identity and the identity of your organization.

All findings from this study will be shared with the first responder community to help inform their continued efforts in the face of COVID-19.

In September 2020, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) partnered with the University of Maryland's START program and Second Sight Training Systems on this three-phase study.

Phase 1 involved a literature review of over 500 research publications related to COVID-19 and interviews with 29 first responders representing 29 distinct agencies across 16 states. Significant preliminary findings from the 29 first responder interviews are summarized in this article by DHS S&T, available

Highlights

from the United States Fire Administration (USFA). More in-depth information on the Phase 1 literature review and additional guidance materials are now available via the study's COVID-19 Topic Dashboard for the First Responder Community.

Phase 2 of the study, currently underway, will involve targeted interviews with first responders on themes that emerged during Phase 1. Additionally, in-depth staffing studies will provide more information on how the pandemic has affected personnel, call volume and service delivery.

For more information or to get in touch with the researchers, please email the DHS program manager, Ross Owens.

If you take a few minutes to complete the short survey, your input will go a long way to help identify best practices that can be implemented now and strategies for the future to make first responder organizations more resilient to pandemics.

(Sources: START, USFA)

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

NIST launches full technical investigation into Champlain Towers South collapse in Surfside, Fla.

The National Institute of Standards and Technology (NIST) is conducting a full technical investigation into what caused the partial collapse of the Champlain Towers South Condominium in Surfside, Florida on June 24.

NIST is currently focused on collecting evidence to support its full investigation, so they are gathering samples of building materials and local soil. NIST experts have also visited the Champlain Towers North condominium to gain a better understanding of the Champlain Towers South building, which had a similar design and construction.

Ongoing search-and-rescue operations are still the highest priority. NIST is working alongside search-and-rescue teams at the site, using non-invasive remote sensing methods for its evidence collection, with the help of technology. These include daily digital captures of the debris pile using lidar scans, time-lapse camera recordings, and drones carrying cameras over the site to help with geotagging of evidence.

The National Construction Safety Teams (NCST) Act of 2002 authorizes NIST to investigate failure of any building that resulted in substantial loss of life or posed significant potential for doing so. Under the NCST Act, NIST is tasked with the responsibility to dispatch teams of experts, where appropriate and practical, within 48 hours after major building disasters.

NIST is now in the process of putting together the National Construction Safety Team that will lead the full technical investigation. The investigation could take years. Once completed, it will hopefully lead to recommendations to improve building codes, standards or practices that could prevent a tragedy like this from happening in the future.

To provide updates to the public, NIST has created a landing page for the Champlain Towers South Collapse on its website. You can visit this page for any future updates on NIST's technical investigation.

(Source: NIST)

Updates to AirNow Fire and Smoke Map equip the public with air quality monitoring as wildfire smoke blankets the US

Last year saw an especially intense wildfire season, and this year is proving to be just as intense, with hotter, drier weather in the Western and Southwestern United States fueling larger and more frequent wildland fires. While the wildfires themselves are predominantly impacting the West and Southwest, smoke from these wildfires is spanning a much bigger area, significantly impacting air quality across the entire U.S.

The current spread of wildfire smoke across the United States highlights how important it is to have up-to-date information on air quality hazards. The Environmental Protection Agency (EPA) and the U.S. Forest Service have just released updates to the popular AirNow Fire and Smoke Map, which provides near-real-time information to enhance awareness of air quality hazards from wildfire smoke. The updates will make this important information more accessible and actionable for users.

EPA and the Forest Service launched the Fire and Smoke Map as a pilot in 2020 to provide the public information on fire locations, smoke plumes and air quality all in one place. The map quickly became a key wildfire smoke information source for the public, with more than 7.4 million views in the map's first three months.

The updated Fire and Smoke Map now includes a dashboard that map users will see by clicking on a monitor or sensor. The dashboard gives users quick access to key information that can help them plan their activities: the current Air Quality Index (AQI) category at the monitor/sensor location; information showing whether air quality is getting better or worse; and information about actions to consider taking, based on the current AQI.

The updated Fire and Smoke Map also is more mobile-friendly for people who visit AirNow.gov from a smartphone or tablet. The map will be available as part of the AirNow app in app stores in the coming weeks.

You can check out the updated AirNow Fire and Smoke Map at the EPA's AirNow.gov website.

(Source: EPA)

Webinar: Community Awareness Briefing on violent extremist recruitment tactics

The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) is hosting a webinar designed to help participants develop an understanding of violent extremist recruitment tactics and explore ways to prevent such threats at the local level.

The goal of this Community Awareness Briefing (CAB) presentation is to raise awareness as to how violent extremist movements recruit individuals to commit violent or illegal acts, negatively impacting these individuals, their families, and their communities. This helps audience members begin to think about possible actions to intervene in a person's radicalization before the line of criminal activity is crossed.

The goal is accomplished by using a series of case studies covering the spectrum of violent extremist groups to illustrate the radicalization and recruitment process, but more importantly to identify vulnerabilities and points of intervention.

Community Awareness Briefings are part of an outreach program from DHS's Center for Prevention Programs and Partnerships (CP3), which replaced the former DHS Office for Targeted Violence and Terrorism in May 2021. CP3 helps build local prevention frameworks that provide communities with the tools they need to combat terrorism and targeted violence.

This webinar will take place on **Thursday, August 12, 2021, from 1:00 to 2:30 p.m. EST**. To register for this webinar, visit the Department of Homeland Security's webinar registration page.

(Source: DHS CISA)

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

Four Chinese Nationals working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including infectious disease research

A federal grand jury in San Diego, California, returned an indictment in May charging four nationals and residents of the People's Republic of China with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018.

The indictment, which was unsealed on Friday [July 16], alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes.

(Source: Department of Justice)

CISA: Alert (AA21-200B) - Chinese State-Sponsored Cyber Operations: Observed TTPs

The National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets.

This Joint Cybersecurity Advisory (CSA) provides information on tactics, techniques, and procedures (TTPs) used by Chinese state-sponsored cyber actors.

Read the full Advisory from NSA, CISA and the FBI.

(Source: CISA)

US State Department offering $10 million reward for state-backed hackers

The State Department announced a $10 million reward for any

information about hackers working for foreign governments.

The measure is aimed squarely at those participating in "malicious cyber activities against US critical infrastructure in violation of the Computer Fraud and Abuse Act." In addition to ransomware, the notice mentions a number of other cyber violations and notes that it applies to government computers as well as "those used in or affecting interstate or foreign commerce or communication."

(Source: ZDNet)

NIST outlines security measures for software use and testing under executive order

The National Institute of Standards and Technology met crucial obligations laid out for it in a May 12 executive order with the publication of documents recommending minimum standards for the verification and use of software in the federal government.

The order was created in response to hackers infiltrating government contractor SolarWinds to distribute malware to thousands of victims, including federal agencies, through what seemed to be a legitimate software update from the IT management firm.

NIST was tasked with identifying security measures for the use of critical software and recommending minimum standards for software vendors to test their products before offering them to the government by July 11 and issued a bulletin linking to the documents on July 9.

(Source: NextGov)

2021 CWE Top 25 Most Dangerous Software Weaknesses

The Homeland Security Systems Engineering and Development Institute, sponsored by the Department of Homeland Security and operated by MITRE, has released the 2021 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list. The Top 25 uses data from the National Vulnerability Database (NVD) to compile the most frequent and critical errors that can lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, obtain sensitive information, or cause a denial-of-service condition.

CISA encourages users and administrators to review the Top 25 list and evaluate recommended mitigations to determine those most suitable to adopt.

(Source: CISA)

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