EMR-ISAC InfoGram Apr. 22 – Arson Awareness Week, May 2-8: Arson during civil unrest; GAO report to Congress on Move Over la

EMR-ISAC sent this bulletin at 04/22/2021 02:30 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 21 — Issue 16 | April 22, 2021

GAO report to Congress on Move Over laws

The Emergency Responder Safety Institute reported numerous struck-by incidents involving emergency responders across the country in the first week of April.

These "struck-by" reports involved an assistant fire chief in Boston, a U.S. Park Police officer in Northwest Washington, D.C., and police officers in Georgia, Rhode Island, Texas, Woodlawn, Maryland, and two in Pikesville, Maryland. Two of these incidents resulted in line-of-duty deaths, including a police officer in Illinois investigating a crash, and a U.S. Capitol Police Officer.

Police, fire, medical, towing, and other responders risk being killed or injured by passing vehicles when responding to a roadside emergency. To protect these vulnerable workers and improve highway safety, all states and the District of Columbia have enacted Move Over laws. Move Over laws vary by state but generally require motorists to move over a lane or slow down, or both, when approaching emergency response vehicles with flashing lights stopped on the roadside.

In December 2020, the United States Government Accountability Office (GAO) released a research study reporting to the United States Congress on the impact of state Move Over laws titled Emergency Responder Safety: States and DOT are Implementing Actions to Reduce Roadside Crashes.

Some of the findings of the report included:

- The U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) data provided limited information on whether crashes involved violations of these state laws.
- State officials cited raising public awareness as the most prevalent challenge, as motorists may not know the law exists or its specific requirements.

To address these challenges, the NHTSA administers funding that states can use for public awareness activities or enforcement initiatives related to emergency responder safety. NHTSA officials are also planning several research efforts intended to enhance emergency responder safety, including studies on motorist behaviors that contribute to roadside incidents and technologies that protect law enforcement officials, first responders, roadside crews and other responders.

The Federal Highway Administration is also supporting the nationwide effort to improve roadside safety with a coordinated network of stakeholders to provide training programs for emergency responders.

(Source: GAO)

Resources and webinar on arson during civil unrest for Arson Awareness Week, May 2-8

The United States Fire Administration (USFA) recognizes Arson Awareness Week on May 2-8, 2021. This year's theme is "arson

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

Awareness Week on May 2-8, 2021. This year's theme is "arson during civil unrest."

The USFA provides resources and guidance on critical actions that first responders must take to help ensure a safe response to arson fires during civil unrest incidents, which endanger the lives of responders and civilians and create devastating fiscal loss for communities.

The USFA is offering a webinar, Arson During Civil Unrest-An Unjustifiable Crime on **May 3, 2021, from 8 a.m. to 11 a.m. EST**. USFA has partnered with seven other organizations to make this event possible. The webinar will include discussions on historic civil unrest responses, mutual aid agreements, risk management, civil unrest response strategies, federal arson statutes and sentencing, and dealing with multiple scenes. To register, visit the USFA website and click "Save Me A Spot."

The USFA and the National Highway Traffic Safety Administration's Office of Emergency Medical Services worked together to compile best practices when responding to civil unrest incidents. Fire and emergency medical services personnel should follow this guidance to prepare personnel, the station, apparatus and the community.

In its Active Assailant Security Resources collection the Cybersecurity and Infrastructure Security Agency (CISA) recently updated its Fire as a Weapon Action Guide, providing guidance to all first responders, security professionals, and the general public to mitigate a potential incident of fire as a weapon. The United States faces increasingly complex threats from terrorism and targeted violence. Historically, assailants have used fire as a weapon to target critical infrastructure, and incidents of fire used as a weapon have increased recently.

(Sources: USFA, CISA)

FEMA updates Resilience Analysis and Planning Tool, expands capabilities for coronavirus planning and response

The Federal Emergency Management Agency (FEMA) has released updates expanding the capabilities of its Resilience Analysis and Planning Tool (RAPT).

The tool is a free-to-use GIS web map allowing federal, state, local, tribal and territorial emergency managers and other community leaders to examine the interplay of census data, infrastructure locations, and hazards, including real-time weather forecasts, historic disasters and estimated annualized frequency of hazard risk.

The updates provide expanded capabilities that can be used specifically for coronavirus pandemic planning and response efforts, including:

- The location and size of infrastructure entities such as hospitals, nursing homes, urgent care facilities, public health departments, and pharmacies.
- Population count and demographics of individuals within a containment zone (e.g. over age 65, disability, educational attainment)

These expanded capabilities are made possible through major updates to data sets and key features, including:

- The most current census tract demographic data from the American Community Survey (five-year data from 2015-2019), including a new data layer on broadband internet access.
- Estimated annualized frequency of 15 hazards at the county-level, drawn from FEMA's National Risk Index analysis.
- New data layers on National Flood Insurance Program policy penetration rates.
- New symbology legends, revised navigation tabs and data display tools that simplify the analysis of community resilience indicators.

The Resilience Analysis and Planning Tool is publicly available at FEMA's website as an ArcGIS web application. The tool is packaged with extensive supporting documentation, including a user guide, a summary list of resilience analysis and planning data layers and sources, a summary of community resilience indicator research and several recently updated video how-to guides.

For questions and feedback, email FEMA-TArequest@fema.dhs.gov.

(Source: FEMA)

FEMA opens application period for emergency management programs

FEMA's Emergency Management Institute (EMI) announces the application period for the National Emergency Management Advanced Academy, the National Emergency Management Executive Academy, and the Master Public Information Officer Program.

Applications for the National Emergency Management Advanced Academy and the National Emergency Management Executive Academy are being accepted from **April 1 through June 1, 2021** for the Fiscal Year (FY) 2022 Cohorts. An announcement of the results will be made to applicants in **August 2021.**

- The National Emergency Management Advanced Academy is designed for Emergency Management mid-level managers with five years of experience in the Emergency Management profession with a significant role directly connected to the Profession of Emergency Management or a recognized EM organization.
- The National Emergency Management Executive Academy is designed for emergency management senior executives in State, Local, Tribal, and Territorial non-governmental organizations (NGOs), academic institutions, and private sector entities. Ideal candidates will serve on major commissions and task forces and/or be responsible for decisions that have a significant effect on policy.

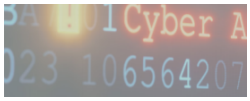
For the Master Public Information Officer Program, applications are accepted from **April 6 to June 1, 2021** for the Fiscal Year (FY) 2022 Cohort. An announcement of the results for this course will be made to applicants in September 2021. The Master Public Information Officer Program is a three-course series that prepares public information officers for an expanded role in delivering public information and warnings using a strategic whole community approach.

For more information on how to apply, visit EMI's website.

(Source: EMI)

National Supply Chain Integrity Month

April is National Supply Chain Integrity Month. In partnership with the Office of the Director of National Intelligence (ODNI), the Department of Defense, and other government and industry partners, CISA is promoting a call to action for a unified effort by organizations across the country to strengthen global supply chains



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

chains.

Information and communications technology (ICT) products and services ensure the continued operation and functionality of U.S. critical infrastructure. However, recent software compromises and other events have shown the far-reaching consequences of these threats. When a supply chain incident occurs, everyone suffers: buyers, suppliers and users.

As the Nation's risk advisor, CISA's top priorities include securing the global ICT supply chain from the evolving risks of tomorrow. Every week, CISA is promoting resources, tools, and information, including those developed by the public-private ICT Supply Chain Risk Management (SCRM) Task Force.

CISA themes for each week include:

- Week 1: Building Collective Supply Chain Resilience
- Week 2: Assessing ICT Trustworthiness
- Week 3: Understanding Supply Chain Threat
- Week 4: Knowing the Essentials

(Source: CISA)

NSA-CISA-FBI Joint Advisory on Russian SVR targeting U.S. and allied Networks

CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national security and government-related systems.

Specifically, SVR actors are targeting and exploiting the following vulnerabilities:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

Additionally the White House has released a statement formally attributing this activity and the SolarWinds supply chain compromise to SVR actors.

(Source: CISA)

China-linked hackers used VPN flaw to target U.S. defense industry researchers

According to cybersecurity researchers, at least two threat groups have spent months taking advantage of a previously undisclosed vulnerability in US virtual private networking (VPN) devices, exploiting the flaw to spy on the US defense industry. Cybersecurity researchers at Ivanti stated that hackers took advantage of the flaw in its Pule Connect Secure suite to break into the systems of a limited amount of customers. A patch for the flaw will likely not come until early May.

Ivanti did not indicate who was behind the espionage campaign, however, FireEye researchers claim that at least one of the hacking groups is backed by the Chinese government. The other, according to researchers, is suspected to have ties to China-based initiatives. FireEye made the connections after conducting a review of the hackers' tools, tactics, targets, and infrastructure.

(Source: OODA Loop)

CISA issues deadline for federal agencies to address Pulse Secure vulnerabilities

Federal agencies have until 5 p.m. EST on April 23 to implement an emergency directive the Cybersecurity and Infrastructure Security Agency issued on vulnerabilities affecting virtual private networking service Pulse Secure Connect, which

virtual private networking service Pulse Secure Connect, which have already compromised federal agencies.

The directive issued Tuesday evening is CISA's third emergency directive this year. Last week agencies were ordered to submit reports to CISA following the release of new patches for on-premises Microsoft Exchange Servers and are now facing new compromises of credentials following intrusions by SolarWinds' hackers that took advantage of their access to legitimate accounts to move around in their networks.

(Source: NextGov)

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