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

The InfoGram

Volume 21 — Issue 25 | June 24, 2021

Resources from USFA and IAFF on mitigating heat stress with firefighter rehabilitation

This week is the 2021 Firefighter Safety Stand Down Week, highlighting critical safety, health and survival issues for fire and emergency services personnel. This year's theme is "Rebuilding Rehab," and one of the most important aspects of firefighter post-incident rehabilitation is mitigating the heat stress inherent in the job of firefighting.

Firefighters work in high-heat conditions, and Personal Protective Equipment (PPE) used in firefighting operations carry a high heat burden. Additionally, extreme heat from environmental conditions, like what is currently scorching the American West, adds significantly to the risk of heat-related health emergencies.

Aside from the acute risks of heat exhaustion and heat stroke, heat stress is also hard on the heart, and the leading cause of firefighter line-of-duty deaths is sudden cardiac events. Research suggests that heat stress may contribute to the likelihood of a sudden cardiac event in those with underlying heart conditions.

According to the United States Fire Administration's (USFA's) guidance on Emergency Incident Rehabilitation, while exposure to extreme heat situations will usually occur in limited, short doses for most firefighters, the effects of high heat on personnel are cumulative.

These factors make it critically important for firefighter health and wellness to perform adequate fitness testing, limit the length of time firefighters are exposed to heat, and provide medical monitoring and effective cooling during post-incident rehabilitation.

The USFA's Emergency Incident Rehabilitation manual is a valuable resource for creating or updating a firefighter rehabilitation program that incorporates all methods available to mitigate heat stress in firefighters. The International Association of Fire Fighters (IAFF) has partnered with the USFA to enhance the manual with additional job aids and training resources, including instructional materials for Firefighter Rehabilitation at Emergency Scenes and Training Exercises, a list of Recommended Minimum Rehab Supplies

Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response –

to Be Carried On Various Apparatus, specs for rehab vehicles, and more.

Visit the USFA's website to access the Emergency Incident Rehabilitation manual, and IAFF's website to take advantage of all the resources supporting the manual. Visit safetystanddown.org for even more resources, including videos and presentations on firefighter rehabilitation.

(Sources: USFA, IAFF, safetystanddown.org)

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

FICEMS releases Telemedicine Framework for EMS and 911

In May 2021, the Federal Interagency Committee on Emergency Medical Services (FICEMS) released a framework which explores the possibility of meeting unmet healthcare needs through telemedicine.

Use of telemedicine in emergency medical services (EMS) and 911 services is still in its infancy. However, adoption and incorporation of telemedicine practices and information into EMS and 911 operations can benefit patients, the EMS and 911 communities and the healthcare delivery systems in which they operate.

While the traditional EMS model of service has focused on emergency medical care at a scene and quick transport to a hospital, this focus is expanding. The pressures and complexities of providing out-of-hospital care during the COVID-19 pandemic have led to an increase in the use of telemedicine in healthcare generally, and has established a new level of service for EMS and 911 systems for providing care to patients.

Another driver contributing to the viability of a telemedicine program for EMS and 911 organizations is its relationship with the new Emergency Triage, Treat, and Transport (ET3) model from the Centers for Medicare and Medicaid Services' (CMS's) Innovation Center (also known as CMMI), implemented earlier this year. Under this model, EMS can now be reimbursed by CMS for 1) transport of a patient to an alternative destination partner, such as a primary care office, urgent care clinic, or a community mental health center (CMHC), or 2) initiation and facilitation of treatment-in-place with a qualified health care partner, either at the scene of the 911 emergency or via telemedicine.

The target audience for this document, Telemedicine Framework for EMS and 911 Organizations, includes EMS and 911 organizations, agencies, and practitioners interested in understanding more about telemedicine practices and options as they relate to out-of-hospital healthcare. The document may be most useful for those organizations that are new to the concepts and considerations of telemedicine and are interested in getting started with a telemedicine program.

The framework offers suggestions for how to engage stakeholders and policymakers and how to assess financial considerations when implementing a program. It also cites and links to a number of other resources, making it a great starting place to learn about telemedicine in EMS and 911 and find more information.

FICEMS' Telemedicine Framework for EMS and 911 is available from the National Highway Transportation Safety Administration's (NHTSA) Office of EMS.

(Source: NHTSA Office of EMS)

FEMA releases NIMS Incident Complexity Guide

Earlier this month, the Federal Emergency Management Agency (FEMA) released the NIMS Incident Complexity Guide: Planning, Preparedness and Training. This Guide supports state, local tribal and territorial (SLTT) jurisdictions in implementing the objectives of the National Incident Management System (NIMS).

The intended audience for this Guide is any Authority Having Jurisdiction (AHJ). This audience includes agencies and organizations at all levels of government, as well as private sector entities and Nongovernmental Organizations (NGO) with emergency management or incident support responsibilities.

The Guide promotes a common understanding within the whole community by using a consistent method to describe incident complexity principles. It provides a standard, repeatable and scalable method of classifying the complexity of an incident, event or exercise. The document defines the distinct incident complexity levels (Types 1 through 5), with specific guidance on how to select incident complexity level for a particular incident. Using the guide, a systematic characterization of an incident's complexity level can be accomplished using the robust set of incident effect indicators provided in the document. A set of corresponding incident management indicators are provided for each complexity level. The incident management indicators outline a scalable response within the Incident Management System.

The Guide is intended for use during planning, preparedness and training efforts. Although it is not intended for use as a decision-making tool during response, AHJs may use it to develop tools for supporting incident response.

(Source: FEMA)

ISAC National Webinar: Incident Response Tabletop - Working with law enforcement and insurers when responding to cyber incidents

No matter how prepared your agency is, managing a cyber incident is an emotional and stressful experience. Emergency Services Sector organizations have the added stress of knowing that a cyberattack can impact their ability to provide essential services to the public during the most critical times.

Responding to a cyber incident is a collaborative effort, and law enforcement will play a key role in a successful response. However, many agencies hold misconceptions about what working with law enforcement entails during response to a cyber incident. While law enforcement can help recover stolen funds, provide decryption keys for ransomware attacks, and assist with insurance and regulator engagement, many firms are concerned that law enforcement will make the event public or even report the event to regulators.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) are hosting a webinar on **Thursday, July 8, 2021, at 2:00 p.m. EST** entitled Incident Response Tabletop: Working with Law Enforcement and Insurers. During the webinar, presenters will run a simplified tabletop exercise to demystify these common law enforcement misconceptions and demonstrate how law enforcement collaborates with agencies to determine attribution, prosecute the threat actors and support your recovery operations.

Attendees will learn about:

- Engaging law enforcement in Incident Response planning and security awareness.
- Accelerating recovery after an attack.
- Navigating financial recovery and insurance claims.

The MS-ISAC, housed under the Center for Internet Security, is the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. state, local, tribal and territorial (SLTT) government entities, whose mission is to improve the overall cybersecurity posture of the nation's SLTT governments through focused cyber threat prevention, protection, response, and recovery.

Register here for this free ISAC National Webinar.

(Source: Center for Internet Security)

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 collaborating with White House on forthcoming zero-trust strategy

The White House is working on a strategy to boost organizations' use of security systems that look for threats within networks, in addition to guarding the perimeter, according to a Cybersecurity and Infrastructure Security Agency (CISA) official.

A May 12 Executive Order gave agencies 60 days to develop zero-trust implementation plans, with a particular focus on cloud migration. The draft model CISA developed consists of five pillars— identity, device, network, application workload and data—with markers along three stages toward achieving a mature zero-trust architecture.

The former CISA Assistant Director for Cybersecurity recommended agencies use CISA's Cybersecurity Quality Services Management Office Marketplace (Cyber QSMO Marketplace) to identify appropriate vendors, and used the event that prompted the executive order—which extended beyond the breach of IT management company SolarWinds—to provide an example of the importance of vendor diversity.

(Source: NextGov)

MITRE adds D3FEND countermeasures to ATT&CK framework

The United States Government's National Security Agency (NSA) on Tuesday, June 22, announced plans to fund the development of a knowledge base of defensive countermeasures for the most common techniques used by malicious hackers. The project, called D3FEND, is available through the non-profit MITRE Corporation as a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques. The primary goal of the initial

D3FEND release is to help standardize the vocabulary used to describe defensive cybersecurity technology functionality.

In a statement, the NSA said D3FEND establishes terminology of computer network defensive techniques and illuminates previously unspecified relationships between defensive and offensive methods. The MITRE Corporation released D3FEND as a complement to its existing ATT&CK framework, which is widely used as the knowledge base of cyber adversary tactics and techniques based on real-world observations.

(Source: Security Week)

Average time to fix critical cybersecurity vulnerabilities is 205 days: report

A new report has found that the average time taken to fix critical cybersecurity vulnerabilities has increased from 197 days in April 2021 to 205 days in May 2021. Security researchers found that organizations in the utility sector had the highest exposure window with their application vulnerabilities. According to the report, more than 66 percent of all applications used by the utility sector had at least one exploitable vulnerability open throughout the year and over 60 percent of applications in the manufacturing industry also had a window of exposure of over 365 days.

The top five vulnerability classes seen over the last three months include information leakage, insufficient session expiration, cross-site scripting, insufficient transport layer protection and content spoofing.

Read the full synopsis from ZDNet, and the monthly Appsec Stats Flash report for April-May from WhiteHat Security.

(Source: ZDNet)

Ransomware attacks decline as gangs focus on lucrative targets

Ransomware attacks fell by 50 percent in Q1 2021 as threat actors shifted from using mass spread campaigns to focusing on fewer, larger targets with unique samples, according to the McAfee Threats Report: June 2021. Researchers noted that the traditional approach of using one form of ransomware to infect and extort payments from many victims is becoming less prominent, mainly because the targeted systems can recognize and block such attempts over time. Instead, they see a trend towards fewer, customized Ransomware-as-a-Service (RaaS) campaigns tailored to larger, more lucrative organizations.

As a result of this shift, the analysis found that the number of prominent ransomware family types declined from 19 in January 2021 to nine in March 2021. The most detected ransomware group in Q1 2021 was REvil, followed by

RansomeXX, Ryuk, NetWalker, Thanos, MountLocker, WastedLocker, Conti, Maze and Babuk strains.

(Source: Infosecurity Magazine)

Tulsa warns of data breach after Conti ransomware leaks police citations

In early May, Tulsa, Oklahoma suffered a ransomware attack that led to the City shutting down its network to prevent the spread of the malware. The attack disrupted Tulsa's online bill payment systems, utility billing, and email, as well as the websites for the City of Tulsa, the Tulsa City Council, Tulsa Police, and the Tulsa 311.

At the time of the attack, it was unknown what ransomware operation was behind the attack on Tulsa. However, yesterday the Conti Ransomware gang claimed responsibility and published 18,938 of the City's files, mainly police citations and internal Word documents. After the leak of data, the City of Tulsa issued a press release warning that personally identifiable information was exposed in the leaked police citations.

(Source: Bleeping Computer)