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

The InfoGram

Volume 21 — Issue 33 | August 19, 2021

Chemical Safety Board releases new video on fatal hydrogen sulfide release

The Chemical Safety Board (CSB) released a safety video on its investigation into a tragic incident at a waterflood station in Odessa, Texas in 2019. A toxic hydrogen sulfide release at the waterflood station fatally injured an employee and his spouse. The incident was preventable if employees had better awareness and training on the safety hazards, and if proper safety measures had been taken.

Hundreds of thousands of people work in oil and gas extraction in the United States. Ensuring their health and safety is a major concern for employers, regulators, trade associations, industry groups and local communities. Many of the facilities associated with the oil and gas extraction industry are in rural and isolated areas, and employees of these facilities often work alone. Hydrogen sulfide is present at many oil and gas production facilities.

While the CSB's safety recommendations from this incident are primarily directed to the employer, the video may serve to build awareness for fire and EMS agencies about the life safety hazards present in jurisdictions with oil and gas processing or production facilities. This awareness could contribute to more effective emergency planning and response for these kinds of incidents.

The CSB reported six safety issues that contributed to the incident:

- Non-use of a personal hydrogen sulfide (H2S) detector.
- Nonperformance of lockout /tagout.
- Confinement of H2S inside pump house.
- Lack of a safety management program.
- Nonfunctioning H2S detection and alarm system.
- Deficient site security.

Videos in the CSB's safety video series have received numerous awards and are often used in training, seminars, board presentations, and other venues as "object lessons in the consequences of inadequate process safety management." This latest video features detailed animation to explain the chemical processes involved in "waterflooding," to a non-technical audience, the characteristics of the site where the incident occurred, and the sequence of events and human errors leading to a fatal hydrogen sulfide gas release.

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

You can check out the video and full investigation report on the CSB's website.

(Sources: CSB, IAFC)

contact the EMR-ISAC office at: (301) 447-1325 and/or fema-emr-isac@fema.dhs.gov.

Subscribe here

CISA releases Public Safety Communications and Cyber Resiliency Toolkit

The ability to maintain voice and data communications is critical for public safety agencies. "Communications resilience" is always a priority. By establishing resiliency measures, public safety communications can better withstand potential disruptions to service.

Many resources are available to assist public safety agencies with communications resilience, but it can be hard to keep up with the abundance of rapidly evolving information. The Cybersecurity and Infrastructure Security Agency (CISA) has addressed this issue with the creation of a Public Safety Communications and Cyber Resiliency Toolkit. The Toolkit is designed to be a living document, with the ability to grow and expand as new resources are developed and identified.

The guidance in the Toolkit serves a number of purposes for public safety agencies: to identify emerging trends and issues, consolidate resources, evaluate current resiliency capabilities, identify ways to improve resiliency, and develop plans for mitigating the effects of potential threats to communications resilience.

CISA has developed an interactive graphic to intuitively index the resources in the Toolkit. Clicking on a topic reveals a list of resources, each with a brief description. Topic areas include essential emergency communications infrastructure such as systems for alerts and warnings, local area networks, and next generation 911 services. Resources in the Toolkit address ways in which these essential communications infrastructures can be disrupted, such as by electromagnetic pulse; jamming; positioning, navigation, and timing disruptions; ransomware, and more. Guidance is offered to improve resilience against these potential threats.

You can read the full news release and access the Public Safety Communications and Cyber Resiliency Toolkit on CISA's website.

(Source: CISA)

FEMA focuses on hazard mitigation in August with historic new funding, grant announcements and training opportunities

August has been an eventful month for the Federal Emergency Management Agency's (FEMA's) hazard mitigation programs.

On August 5, the Biden Administration committed $3.46 billion in hazard mitigation funds to reduce the effects of climate change. Through its Hazard Mitigation Grant Program (HMGP), FEMA will now administer this historic level of funding to states, tribes, and territories. This one-time investment represents a 23% increase in the funding made available for declared disasters since the program's inception. Every state, tribe, and territory that received a major disaster declaration in response to the COVID-19 pandemic will be eligible to receive 4% of those disaster costs to invest in mitigation projects that reduce risks from natural disasters. You can view the breakdown of how this $3.46 billion in HMGP funding will be allocated to each state on FEMA's website.

On August 9, FEMA announced Notices of Funding Opportunities (NOFOs) for two competitive hazard mitigation assistance grant programs for fiscal year 2021, providing an additional $1.16 billion in hazard mitigation assistance funding to states, tribes and territories.

- The Building Resilient Infrastructure and Communities (BRIC) grant program will allocate $1 billion to support communities' capability- and capacity-building; encourage and enable innovation; promote partnerships; enable large projects; maintain flexibility; and provide consistency. Scoring criteria for this year's program has been adjusted to incentivize mitigation actions that consider climate change and future conditions, populations impacted and economically disadvantaged rural communities, in line with the Biden administration's Justice40 Initiative.

- The Flood Mitigation Assistance (FMA) grant program will make $160 million available for projects that reduce or eliminate the risk of repetitive flood damage to buildings and structures insured by the National Flood Insurance Program. FMA will use the Centers for Disease Control and Prevention's Social Vulnerability Index as a selection factor in its competitive scoring process. This means underserved populations will receive more points for projects that benefit their communities.

FEMA is offering a series of webinars providing more information and technical assistance on how to apply for the BRIC and FMA grants. Recordings of past webinars are also available via the same webpage where upcoming webinars are listed. Applications for both for BRIC and FMA grants must be submitted on Grants.gov by **September 30, 2021.** Interested applicants should contact their hazard mitigation officer for more information.

Many courses in FEMA's Emergency Management Institute (EMI) Mitigation curriculum directly support the training requirements of federal programs, such as the National Flood Insurance Program (NFIP). Participants in these courses learn about program regulations and policies and are provided with the tools and techniques for implementing mitigation strategies. FEMA highlights two courses this month that directly address hazard mitigation projects. These courses can assist in planning eligible projects and applying for hazard mitigation assistance:

- K0219 Mitigation Assessment Team (MAT) Workshop.

- K0212 Hazard Mitigation Assistance: Developing Quality Application Elements Course.

You can apply for these courses on FEMA's website. For more information, contact EMI's Mitigation Branch at (301) 447-1152 or by email at fema-emi-mit@fema.dhs.gov.

(Source: FEMA)

Intermediate Incident Command System (ICS 300) training available in blended, virtual format

FEMA's Emergency Management Institute (EMI) recently announced a new delivery format for its ICS 300 training. Up until now, EMI has offered ICS 300 training only as a fully instructor-led, 3-day (21 hour) course requiring on-site attendance at a local training facility or in residence at EMI. However, it is now available in a blended, asynchronous format and can be attended virtually.

ICS 300, entitled "Intermediate Incident Command System for Expanding Incidents," is part of FEMA's National Incident Management System (NIMS) core curriculum in its NIMS training program. It is intended for individuals who need training on advanced application of the incident command system. Typically, these individuals are those who would be designated as Incident Command System (ICS) or emergency operations center (EOC) leaders or supervisors for large or complex incidents that extend beyond a single operational period and generate an Incident Action Plan (IAP). This course builds upon information covered in the ICS 100, 200, 700 and 800 courses.

The District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA) developed this blended asynchronous version of ICS 300, and EMI has validated the course as meeting all requirements in the Program of Instruction. You can view EMI's ICS 300 course description and objectives via its online training catalog.

This virtual course uses self-paced online trainings and assignments (approximately 14 hours) and a single "live" session of virtual instructor-led training (VILT) that focuses on group discussion and activities (approximately 7 hours). This delivery method requires jurisdictions to establish several technical and administrative processes to make the course functional.

Implementing agencies should determine how to deliver and manage the course in this new format.

State, local, tribal and territorial training points of contact and federal training partners can access these course materials through EMI's Field Delivery Course website. If you are a State Training Officer and need information or access to the Field Delivery Course web site, please contact FEMA-G-Courses@fema.dhs.gov. For all other inquiries, please go to EMI's State Training Officer Contact List.

(Source: EMI)

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

BadAlloc vulnerability affecting devices incorporating older BlackBerry QNX products

CISA released an Alert on August 17 on devices incorporating older versions of multiple BlackBerry QNX products affected by a BadAlloc vulnerability. A malicious actor could exploit this vulnerability to take control of an affected system or cause a denial-of-service condition.

Because devices incorporating older versions of BlackBerry QNX products support critical infrastructure and national critical functions, CISA is strongly urging all organizations whose devices use affected QNX-based systems to immediately apply the mitigations provided in CISA Alert AA21-229A and Blackberry Advisory QNX-2021-001.

(Source: CISA)

Half of US hospitals shut down networks due to ransomware

Nearly half (48%) of US hospitals have disconnected their networks in the past six months due to ransomware, according to a new study from Philips and CyberMDX. The Perspectives in Healthcare Security Report is based on interviews with 130 IT and cybersecurity hospital executives and biomedical engineers and technicians. Respondents who admitted to shutting down networks due to ransomware were a mix of those who did so proactively to avoid a damaging breach and those forced to do so because of severe malware infection.

Of respondents that experienced a shutdown due to external factors, large facilities suffered an average of 6.2 hours downtime at the cost of $21,500 per hour. In comparison, mid-size hospitals averaged nearly 10 hours at $45,700 per hour. More concerning still is that many hospitals still appear to be exposed to severe legacy vulnerabilities.

Nearly two-thirds (65%) of respondents claimed they rely on manual methods to calculate inventory, with many of those from mid-size hospitals (15%) and large hospitals (13%) admitting they have no way to determine the number of active or inactive devices on their networks.

(Source: Infosecurity Magazine)

DOD looks for answers on GPS data spoofing

The Defense Department is looking for solutions that would prevent the growing threat of location data spoofing that can affect satellite-based technology like global positioning systems. The Defense Innovation Unit (DIU) published a solicitation looking for commercial solutions that can help sniff out potential global navigation satellite system disruptions, particularly those that result in "falsified" or spoofed location data across large areas.

The Department of Transportation is working with the DOD and interagency on a national PNT architecture to better understand the threat environment, infrastructure needs and collaboration.

The DIU is looking for technologies that can provide a "near-real-time, common operating picture" and is requesting solutions be submitted by Aug. 23.

(Source: Federal Computer Week)

CISA provides recommendations for protecting information from ransomware-caused data breaches

CISA has released the fact sheet Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches to address the increase in malicious cyber actors using ransomware to exfiltrate data and then threatening to sell or leak the exfiltrated data if the victim does not pay the ransom. These data breaches, often involving sensitive or personal information, can cause financial loss to the victim organization and erode customer trust.

The fact sheet provides information for organizations to use in preventing and responding to ransomware-caused data breaches. CISA encourages organizations to adopt a heightened state of awareness and implement the recommendations listed in this fact sheet to reduce their risk to ransomware and protect sensitive and personal information. Review StopRansomware.gov for additional ransomware resources.

(Source: CISA)

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