U.S. Fire Administration | FEMA

EMR-ISAC InfoGram Jan. 20 – FEMA Fire Prevention and Safety Grant application period now open; Brief outlines Law Enforcement-Mental Health Learning Site Program

EMR-ISAC sent this bulletin at 01/20/2022 04:46 PM EST

View as a webpage / Share

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

The InfoGram

Volume 22 — Issue 3 | January 20, 2022

FEMA Fire Prevention and Safety Grant application period now open

The Federal Emergency Management Agency (FEMA) has released the funding notice for $46 million available through the Fiscal Year 2021 Fire Prevention and Safety (FP&S) grants. These grants are part of the Assistance to Firefighters Grants Program and focus on reducing injury and preventing death among high-risk populations.

The FP&S Program provides financial assistance directly to eligible fire departments, national, regional, state, local, tribal and non-profit organizations such as academic (e.g., universities), public health, occupational health, and injury prevention institutions for fire prevention programs. The program also supports firefighter health and safety research and development such as clinical studies that address behavioral, social science, and cultural research.

Examples of research and development grants and descriptions of completed projects that have been funded under this program can be found on FEMA's website.

The application period opened on **Jan. 18** and closes at **5 p.m. EST on Feb. 18**.

FEMA will host a series of webinars to provide an overview of the FY 2021 FP&S Program and assist with navigating the grant application. The upcoming webinar schedule is as follows:

- FY 2021 FP&S Research and Development Activity - **Friday, Jan. 21, 2 – 3:30 p.m. EST**.
- FY 2021 FP&S Activity - **Wednesday, Jan. 26, noon - 1:30 p.m. EST**.
- FY 2021 FP&S Activity - **Tuesday, Feb. 1, 1 - 2:30 p.m. EST**.
- FY 2021 FP&S Activity - **Wednesday, Feb. 9, 3 – 4:30 p.m. EST**.

Advanced registration is not required for these webinars. Webinar sessions will be broadcast using an Adobe Connect webinar link. FEMA suggests saving this link to your web browser's favorites:

- https://fema.connectsolutions.com/fy21fpswebinars/.

A conference line will also be available at 800-320-4330, Conference Code: 258436.

The funding notice and application assistance documents for this grant program are available at grants.gov and FEMA.gov. For questions, contact FEMA's Fire Grants HelpDesk via email at firegrants@fema.dhs.gov.

(Source: FEMA)

Highlights

FEMA Fire Prevention and Safety Grant application period now open

New brief outlines Law Enforcement-Mental Health Learning Site Program from CSG Justice Center

FEMA launches National Resource Hub, a suite of tools to assist with resource management preparedness

Ethanol Emergency Response training updated with new video series from Renewable Fuels Association

Cyber Threats

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

New brief outlines Law Enforcement-Mental Health Learning Site

Program from CSG Justice Center

Jurisdictions around the country are exploring strategies to improve the outcomes of encounters between law enforcement and people who have mental health needs.

The Council of State Governments Justice Center (CSG Justice Center), with support from a team of national experts and the U.S. Department of Justice's (DOJ's) Bureau of Justice Assistance (BJA), just released a new brief with updated information on its Law Enforcement-Mental Health Learning Site Program. This program is a national resource for law enforcement and behavioral health agencies looking to tailor response models and implementation strategies to their community's needs.

Comprising sheriffs' offices, metropolitan police departments, rural justice and mental health coalitions, and university police departments, the 14 learning sites have been selected through a competitive application process based on their programmatic success in implementing successful police-mental health collaborations. These learning sites offer a wide range of expertise and a variety of model programs, such as crisis intervention training, co-responder models with follow-up teams, comprehensive dispatcher training, embedded mental health professionals, and police officers trained as mental health liaisons.

The CSG Justice Center began the program in 2010 to connect public safety personnel with peers who have successfully planned and implemented innovative response models. Since then, it has continued to expand and regularly deliver assistance and training to law enforcement and mental health practitioners nationwide. Since 2020, the Law Enforcement Mental Health Learning Sites have responded to just over 500 requests for assistance from 38 states in developing such programs tailored to individual community needs and resources.

The CSG Justice Center manages and provides staff support to the learning sites and develops resources that can be tailored to the distinct needs of jurisdictions. CSG Justice Center staff work closely with the learning sites to help match the expertise and resources each site offers to the needs of law enforcement agencies. Those interested are encouraged to contact the learning sites directly and provide notice of your request to le-mh-learningsites@csgjusticecenter.org for tracking purposes.

The new program brief shares additional information on the program's features; a list of the 14 learning sites and their individual services; and links to access more resources, including a Police Mental Health Collaboration Self-Assessment Tool.

For more information, see the CSG Justice Center's 2-page Law Enforcement Mental Health Learning Sites Program Overview, available on the DOJ BJA's website.

(Source: CSG Justice Center)

FEMA launches National Resource Hub, a suite of tools to assist with resource management preparedness

This month, the Federal Emergency Management Agency (FEMA) launched a new National Resource Hub to support communities in implementing the resource management preparedness process defined in the National Incident Management System (NIMS) and the National Qualification System (NQS).

The National Resource Hub serves as a no-cost solution for all state, local, tribal, and territorial government agencies, non-governmental organizations, and other mission partners.

The National Resource Hub is available as part of FEMA's Preparedness Toolkit (PrepToolkit). It is a suite of web-based tools, consolidating the existing Resource Typing Library Tool and OneResponder, as well as a newly launched, centralized, and cloud-hosted Resource Inventory System.

- The Resource Typing Library Tool provides an online library of all resources typing definitions, job titles/position qualification sheets, and position task book (PTB) templates that have been released by FEMA as a part of the NIMS and NQS.
- One Responder provides a solution for organizations and responders to manage personnel qualifications and training history as part of implementing a qualifications and credentialing management process consistently with the NQS.
- The Resource Inventory System provides a solution for organizations to inventory and identify resources and personnel, consistently with NIMS resource typing definitions and job titles/position qualification sheets.

To support the launch of the National Resource Hub, FEMA is hosting a series of educational webinars:

- National Resource Hub Introduction on Jan. 24 and Feb. 8.
- Resource Inventory System Introduction on Feb. 15 and March 15.
- OneResponder and the Course Equivalency Tool Introduction on March 8 and March 22.

For more information and to register for any of these webinars, visit FEMA's National Resource Hub events page.

(Source: FEMA)

Ethanol Emergency Response training updated with new video series from Renewable Fuels Association

Over 16 billion gallons of ethanol are produced in the United States per year and ethanol is one of the top hazardous materials shipped by rail today. Although more than 99.99 percent of hazardous materials are loaded, shipped, transported and unloaded safely, incidents do occur, especially during transportation and transfer of these materials. Just this month, a 98-car train carrying ethanol derailed near the Texas-Oklahoma border. Twenty-five of the 28 derailed cars reportedly caught fire, forcing multiple fire crews from various agencies to respond to battle the blaze and prevent grass fires. The incident was treated as a hazmat situation.

Trained responders are essential to the safety of the many communities across the nation who may see ethanol and other hazardous materials transported through their jurisdictions.

The Renewable Fuels Association (RFA) has just released a new eight-episode video package on ethanol emergency response, developed in conjunction with Transportation Community Awareness Emergency Response (TRANSCAER) and funded via a federal Pipeline and Hazardous Materials Safety Administration (PHMSA) ALERT grant.

The new video series serves to update the RFA's Ethanol Emergency Response training course. The complete set of updated course materials are available from both RFA and TRANSCAER.

Ethanol Emergency Response is offered in several formats:

- Online self-study, no credit: Take the course on RFA's website, or TRANSCAER's website at your own pace.
- Online self-study, for credit: Take the course on TRANSCAER's Learning Management System at your own pace and complete the course evaluation.
- Instructor led, virtual: Attend one of TRANSCAER's upcoming virtual offerings of the course.
- Instructor led, in-person: Attend one of the upcoming in-person offerings of the course, or by contacting your Regional or State TRANSCAER Coordinator to find out more about available opportunities or to arrange a training in your area.

If you or someone in your agency is interested in becoming qualified to deliver this course to emergency responders, TRANSCAER is also offering several upcoming train-the-trainer webinars on Ethanol Emergency Response, scheduled for March 22, June 7 , and Aug. 23, 2022.

Visit TRANSCAER's website for more information on this course and many additional free training opportunities for response to a variety of hazardous materials transportation incidents.

(Source: TRANSCAER, RFA)

Cyber Information and Incident Assistance Links

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

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

StopRansomware.gov

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

CISA urges organizations to implement immediate cybersecurity measures to protect against potential threats

In response to recent malicious cyber incidents in Ukraine—including the defacement of government websites and the presence of potentially destructive malware on Ukrainian systems—CISA has published CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats. The CISA Insights strongly urges leaders and network defenders to be on alert for malicious cyber activity and provides a checklist of concrete actions that every organization—regardless of sector or size—can take immediately to:

- Reduce the likelihood of a damaging cyber intrusion.
- Detect a potential intrusion.
- Ensure the organization is prepared to respond if an intrusion occurs.
- Maximize the organization's resilience to a destructive cyber incident.

(Source: CISA)

Oracle releases January 2022 Critical Patch Update

Oracle has released its Critical Patch Update for January 2022 to address 497 vulnerabilities across multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the Oracle January 2022 Critical Patch Update and apply the necessary updates.

(Source: CISA)

Microsoft warns of destructive malware targeting Ukrainian organizations

Microsoft has released a blog post on possible Master Boot Record (MBR) Wiper activity targeting Ukrainian organizations, including Ukrainian government agencies. According to Microsoft, powering down the victim device executes the malware, which overwrites the MBR with a ransom note; however, the ransom note is a ruse because the malware actually destroys the MBR and the targeted files. CISA recommends network defenders review the Microsoft blog for tactics, techniques, and procedures, as well as indicators of compromise related to this activity. CISA additionally recommends network defenders review recent Cybersecurity Advisories and the CISA Insights, Preparing For and Mitigating Potential Cyber Threats.

(Source: CISA)

FBI Industry Alert: Indicators of Compromise Associated with Diavol Ransomware

The FBI first learned of Diavol ransomware in October 2021. Diavol is associated with developers from the Trickbot Group, who are responsible for the Trickbot Banking Trojan. Diavol encrypts files solely using an RSA encryption key, and its code is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. While ransom demands have ranged from $10,000 to $500,000, Diavol actors have been willing to engage victims in ransom negotiations and accept lower payments. The FBI has not yet observed Diavol leak victim data, despite ransom notes including threats to leak stolen information.

(Source: FBI Internet Crime Complaint Center – IC3)

FBI PSA: Cybercriminals tampering with QR Codes to steal victim funds

The FBI is issuing this public service announcement (PSA) to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with QR codes to redirect victims to malicious sites that steal login and financial information.

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

(Source: FBI Internet Crime Complaint Center – IC3)