U.S. Fire Administration | FEMA

EMR-ISAC InfoGram Dec. 16 – NIOSH requests input on personal protective technology research and practice needs; NIST Voices of First Responders data on communication technology needs now available in new Usability Results Tool

EMR-ISAC sent this bulletin at 12/17/2021 11:15 AM EST

View as a webpage / Share

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

The InfoGram

Volume 21 — Issue 49 | December 16, 2021

NIOSH requests input on personal protective technology research and practice needs, comments due Jan. 31

The National Institute for Occupational Safety and Health (NIOSH), within the Centers for Disease Control and Prevention (CDC), is soliciting public comment on the need to establish centers of excellence to address research and practice needs in the area of personal protective technology (PPT), including personal protective equipment. The centers of excellence would serve as knowledge hubs where experts from multiple disciplines, industry representatives, and other interested parties/groups collaborate on PPT research and practice.

NIOSH is seeking input from any interested party regarding the scope of these future centers of excellence. Potentially, these centers could play roles in identifying research needs, conducting research, disseminating information including education and outreach activities, and translating research findings and technologies into products and practices that will enhance safety and health.

The NIOSH National Personal Protective Technology Laboratory has identified the following three broad focus areas to be addressed by one or more future centers of excellence:

- Research and development of new technologies and approaches to PPT, including sensor technology to increase efficacy.
- Research to evaluate the factors that influence the

Highlights

adoption and usage of PPT such as performance, comfort, fit, and usability; health and safety management systems, safety culture, and regulatory requirements.

- Research into innovative approaches to the design, manufacture, and maintenance of PPT that enhance factors such as the effectiveness and acceptance of PPT in varied user populations, availability and the ability to rapidly customize and produce PPT during crises.

In addition to input on the three topic areas, NIOSH is seeking input on a number of questions. See the full document in the Federal Register for more information.

Comments are due by **Jan. 31, 2022** and may be submitted via either of the following two methods:

- The Federal eRulemaking Portal (follow the instructions for submitting comments).
- Send mail to: NIOSH Docket Office, 1090 Tusculum Avenue, MS C-34, Cincinnati, Ohio 45226-1998.

(Source: Federal Register)

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 Voices of First Responders data on communication technology needs now available in new Usability Results Tool

Over the past several years, the National Institute of Standards and Technology (NIST) Public Safety Communications Research (PSCR) Division has been conducting a Usability and User Interface project assessing emergency responder communication technology needs through extensive interviews and surveys. NIST recently made the project's entire data set available to the public, accessible and downloadable within a new web-based data visualization and analysis tool called the Usability Results Tool.

To date, the project has progressed through two phases.

Phase 1 consisted of a series of in-depth interviews with approximately 200 first responders on their views of communication technology. Findings from Phase 1 concluded that first and foremost, responders wanted their communication technology to be reliable. Their primary need for their communication technology was for solutions to their current problems, rather than development of new technology. Many were also interested in communication technology that can provide them with real-time information. Additionally, first responders wanted improved interoperability with other disciplines, agencies, and jurisdictions.

Phase 2 used the Phase 1 results to inform a nationwide survey of over 7,000 first responders within the 911/dispatch, emergency medical services (EMS), fire service, and law enforcement disciplines. The Phase 2 nationwide survey confirmed and expanded on the needs and problems related to communication technology identified in interviews during Phase 1.

The NIST PSCR Usability Team recently provided public access to the data from these interviews

and surveys by creating the PSCR Usability Results Tool: Voices of First Responders. Over 20,000 first responder quotes from the first responder interview data, as well as the 7,182 survey responses are available within the tool.

The Usability Results Tool provides a means to analyze the survey results and create charts and tables dynamically based on filter selections. Survey results accessed via the Survey Results Tool, the Survey Analyzer Tool, and the interview quotes, available via the Interview Quotes Tool, can be freely used to influence the research, design and development of communication technology in the public safety domain. Any interview quotes or survey results used in published materials should properly attribute this tool as well as the appropriate reports.

NIST PSCR provided a review of the results from this multi-year research study, including an overview of the new Usability Results Tool, during its PSCR 2021: The Digital Experience virtual conference, held in June this year. NIST has posted the presentation slides and a video recording of this session on its website.

NIST PSCR has also published a series of reports interpreting and summarizing the results of this multi-year research study. To access NIST's Voices of First Responders report series, visit NIST PSCR's User Interface/ User Experience Publications page.

For more information about the NIST PSCR Usability Team research, or for questions regarding the PSCR Usability Results Tool, please send an email to usability@nist.gov. More information about the PSCR program can be found at pscr.gov.

(Source: NIST)

FEMA updates Long-Term Community Resilience Exercise Resource Guide to assist with climate-focused exercises

The impacts of climate change are being felt today in communities across the country and increasingly test community resilience. Exercises provide a forum for participants across the whole community to discuss and better understand climate change and plan for, adapt to and mitigate their risks and hazards.

Exercise scenarios, modeling and simulations tangibly represent how climate change will increase the need for resources while diminishing capabilities. Participation in exercises provides a common understanding of community risk; current and planned programs related to community resilience; and critical issues relevant to future community planning.

In November 2021, the Federal Emergency Management Agency (FEMA) released its Long-Term Community Resilience Exercise Resource Guide: Designing Whole Community Exercises to Prepare for the Effects of a Changing Climate. The Guide equips users with:

- A dictionary with common terms to ensure a shared understanding of climate-related terminology and principles before an exercise.
- Tools and templates for planning and conducting climate-focused exercises.
- Resources including funding opportunities, risk assessments and training programs.

Any jurisdiction, organization, network or regional coalition can use this Guide to continually improve its collective resilience, and the resilience of the community and nation, in the face of real and rising climate change vulnerabilities, threats and impacts.

The Guide offers the latest Homeland Security Exercise and Evaluation Program (HSEEP) guiding principles, new discussion prompts specific to climate change and social justice, and noteworthy

resources from across the interagency.

The updated Guide is available for download on FEMA's website and FEMA's Preparedness Toolkit website, along with its companion resource of historical reference documents, consisting of a collection of historical Exercise Seminar Participant and Situation Manuals.

Please e-mail FEMA's National Exercise Division at NEP@fema.dhs.gov with any questions or to share how you are using the Long-Term Community Resilience Exercise Resource Guide.

(Source: FEMA)

NFPA releases free drone training and Drone Knowledgebase for public safety agencies

The use of unmanned aircraft systems (UAS), also known as drones, in firefighting operations is on the rise. Public safety agencies can use drones to support a wide variety of operations in structural and wildland firefighting, search and rescue, hazardous materials, natural disasters, active shooter events, and any response requiring increased situational awareness. However, public safety drone users are often operating with a lack of general knowledge, planning, and education that can result in accidents, injuries, life-saving operations delays, interference with other aircraft, and exposure to liability.

To address this need, the National fire Protection Association (NFPA) was awarded a Fire Prevention and Safety Grant in 2019 by the Federal Emergency Management Agency (FEMA), as part of its Assistance to Firefighters Grant (AFG) program. Through this initiative, the NFPA is providing training to responders, maintaining a database tracking fire service drone programs and usage, and building an online portal that agencies can use to ensure their drone programs are compliant with current regulations and standards.

As part of this AFG-funded project, in October 2021, the NFPA released a training program, entitled NFPA® Public Safety Drone Guide Online Training, to help fire departments across the United States improve existing public safety drone programs and establish new drone initiatives.

This free online training offers instruction and best practices for the proper administration, operation, and maintenance of a public safety drone program. The training is based on NFPA 2400, Standard for Small Unmanned Aircraft Systems (sUAS) Used for Public Safety Operations, as well as the Federal Aviation Administration's (FAA) Requirements (part 107, 91) and the Code of Federal Regulations — Aeronautics and Space (Title 14 CFR).

The training can be completed at your own pace but is estimated to take about 4 hours. It was custom-built by the NFPA with an intuitive web-based and mobile-friendly interface. Features of the training include gamified content, 360-degree video, immersive virtual reality (VR) tools including 3D simulations with the option to view using a mobile VR headset, and an "action planner," allowing for documentation of answers to key questions as participants progress through the course.

In addition to the free training, in December 2021, the NFPA released its Drone Knowledgebase, which will promote information sharing and collaboration among U.S. public safety entities that have established drone programs and those seeking to form programs. The Drone Knowledgebase is expected to become more robust as fire departments learn about the resource, contribute local information, and invite neighboring jurisdictions to add their program details.

The NFPA has established a dedicated landing page, nfpa.org/drones, so that members of the fire service can access the 4-hour training, NFPA 2400, a training teaser video, research, related content, and the Knowledgebase in one convenient location.

(Source: NFPA)

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

MS-ISAC URGENT MESSAGE: Log4j zero-day vulnerability response

On Dec. 9, security researchers discovered a flaw in the code of a software library used for logging. The software library, **Log4j**, is built on a popular coding language, Java, that has widespread use in other software and applications used worldwide. This flaw in Log4j is estimated to be present in over 100 million instances globally.

The flaw, also known as a *vulnerability* by the security community, was rated a 10 out of 10 on the Common Vulnerability Scoring System, or CVSS, due to the potential impact that it can have if leveraged by attackers. The confirmed affected versions of Log4j are **2.0-beta-9 through 2.14.1**.

Due to the widespread prevalence of Log4j, the high impact of an attack against it, and evidence that malicious actors are actively targeting organizations with vulnerable versions of Log4j, **the Center for Internet Security (CIS) is encouraging all organizations to mitigate risk as soon as possible**.

It is important to note that simply updating Log4j may not resolve issues if an organization is already compromised. In other words, updating to the newest version of any software will not remove accesses gained by adversaries or additional malicious capabilities dropped in victim environments.

Threat-focused security organizations have observed state actors begin to leverage the vulnerability in new attacks. CIS recommends heightened vigilance in monitoring networks for abnormal behaviors and invoking immediate response actions as necessary.

This page from the Multi-State Information Sharing and Analysis Center (MS-ISAC) is intended to help all organizations, regardless of technical maturity, to find resources for mitigating risks associated with Log4j.

(Source: MS-ISAC)

CISA creates webpage for Apache Log4j vulnerability CVE-2021-44228

CISA and its partners, through the Joint Cyber Defense Collaborative, are tracking and responding to active, widespread exploitation of a critical remote code execution vulnerability (CVE-2021-44228) affecting Apache Log4j software library versions 2.0-beta9 to 2.14.1. Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system.

In response, CISA has created a webpage, Apache Log4j Vulnerability Guidance and will actively

In response, CISA has created a webpage, Apache Log4j Vulnerability Guidance and will actively maintain a community-sourced GitHub repository of publicly available information and vendor-supplied advisories regarding the Log4j vulnerability. CISA will continually update both the webpage and the GitHub repository.

CISA urges organizations to review its Apache Log4j Vulnerability Guidance webpage and **upgrade to Log4j version 2.15.0, or apply the appropriate vendor recommended mitigations immediately**. CISA will continue to update the webpage as additional information becomes available.

(Source: CISA)

Kronos hit with ransomware, warns of data breach and 'several week' outage, affects state and local governments

HR management platform Kronos has been hit with a ransomware attack, revealing that information from many of its high-profile customers may have been accessed.

Ultimate Kronos Group (UKG), Kronos' parent company, said the vital service will be out for "several weeks" and urged customers to "evaluate and implement alternative business continuity protocols related to the affected UKG solutions."

The statement comes hours after the company posted a message on the Kronos community message board, explaining that staff noticed "unusual activity impacting UKG solutions using Kronos Private Cloud" on Saturday night. This private cloud houses data for UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions.

The City of Cleveland sent out an urgent message on Monday, telling WKYC that UKG contacted them and other clients to tell them that the ransomware attack may have compromised employee information like names, addresses, social security numbers, and employee IDs.

The Virginia Department of Behavioral Health and Developmental Services on Tuesday announced it had also been affected by [the UKG] ransomware attack. Virginia uses Kronos to manage its HR functions and in a statement to the Richmond Times-Dispatch on Tuesday said that the ransomware attack on the provider has “paralyzed” its IT system for managing employee payroll and time sheets.

The attack has affected many other public agencies and institutions, including in the governments of West Virginia; Cleveland, Ohio; Tallahassee, Florida; and Springfield, Massachusetts.

(Sources: ZDNet, StateScoop)

Maryland health department faces second week of disruption from cyberattack

Maryland’s health department has not released coronavirus case rates for a ninth straight day because of a cyberattack.

Meanwhile, department employees on Monday, Dec. 13, remained unable to access their computers or many portions of the agency’s network, according to records and interviews, and the disruptions were being felt by local health workers trying to stem the spread of the coronavirus — especially as the new omicron variant was discovered in the state.

Local public health workers gave varying accounts Monday of the severity of problems they faced from the situation. The lack of information has made it difficult or impossible to identify trends of new cases in places such as schools and nursing homes.

(Source: The Washington Post)

Top 10 Malware November 2021

Top 10 Malware November 2021

In November 2021, the Top 10 stayed consistent with the previous month with the exception of Gh0st, Mirai, and Ursnif, which returned to the Top 10. The Top 10 Malware variants comprise 69% of the total malware activity in November 2021, decreasing 2% from October 2021. Shlayer and CoinMiner continue to lead the Top 10 Malware and are likely to continue their prevalence in the Top 10 Malware for the coming months. The MS-ISAC also received a marked increase in Jupyter alerts over the past 6 months, with Jupyter alerts increasing an average of 9% over the past 6 months.

Read the full report from the MS-ISAC.

(Source: MS-ISAC)

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