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

The InfoGram

Volume 21 — Issue 23 | June 10, 2021

New NFPA 1802 Standard establishes specifications for rugged portable radios in the hazard zone

The National Fire Protection Association (NFPA) recently released a new standard, NFPA 1802: Standard on Two-Way, Portable RF Voice Communications Devices for Use by Emergency Services Personnel in the Hazard Zone.

Ten years ago this month, in June 2011, two firefighters were tragically killed in the line of duty while fighting a residential fire in San Francisco, California. Their portable radios and remote speaker microphones (RSMs) failed due to exposure to heat from the fire. They couldn't transmit a mayday that they were trapped.

The National Institute for Occupational Safety and Health (NIOSH) fire fighter fatality investigation report on this tragic incident recommended continued research and efforts to improve radio system capabilities. This led to the development of the new NFPA 1802 Standard, initiated in 2013 and finalized this year.

The new NFPA 1802 Standard defines the parameters for an extremely rugged radio and speaker microphone capable of performing in hostile environments that firefighters, hazardous materials teams, or other personnel that operate in a hazard zone work in.

The Standard is very wide-ranging and is organized around three areas of portable radio design: ergonomics, feature set and environment. Radio frequency (RF) devices and RSMs that meet the NFPA 1802 standard will have to pass unprecedented durability testing and include a data-logging capability. Some of the environmental testing criteria include continuing to operate in 500-degree oven temperatures for five minutes as well as multiple cycles of a 350-degree oven for 15 minutes and subsequent water quench.

These stringent requirements in the new NFPA Standard offer fire fighters new levels of ruggedness, ease of use and improved voice quality and functionality, which will all lead to improved safety in the hazard zone. However, the new requirements also set a challenging benchmark for vendors.

Departments and personnel should understand basic radio principles to remain safe on the fireground and use

Highlights

U.S. Fire Administration

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

communications equipment effectively. Consult the United States Fire Administration's Voice Radio Communications Guide for the Fire Service for a comprehensive resource on this topic.

For more information on the new NFPA 1802 Standard, visit NFPA's website.

(Source: Firehouse)

Tennessee board reports Nashville bombing impact on 911, future plans

Since the December 25, 2020 bombing in downtown Nashville impacted AT&T's regional communications infrastructure and resulted in extended outages for public safety answering points (PSAPs) throughout the state, the Tennessee Emergency Communications Board (TECB) has been working with AT&T to ensure a more resilient 911 network.

The TECB met with AT&T in April and May of this year to discuss what went wrong, and the TECB Vice Chairman presented key findings in a report to the TECB on May 5. Sensitive information, such as that pertaining to network security, was not disclosed publicly, but a recording of the May 5 presentation has been made publicly available.

The outages affected 66 PSAPs for more than four days (more than 97 hours). Power was lost to the AT&T facility at 11:50 a.m. on Christmas Day, and the facility came back online on Dec. 29 at 12:25 p.m. Making matters worse, some 911 centers did not receive notifications or updates about the issue for six days. PSAPs did not receive updates sent from AT&T's Everbridge alerting system because the alerting system had also been damaged.

The TECB report includes some analysis of the factors contributing to the extended outages, impacts to the 66 PSAPs, and actions AT&T will take to avoid outages in the future. The main cause of the 911 outages stemmed from the fact that the AT&T personnel were not allowed to provide supplemental power sources to the key network in a timely manner. This was due to the fact that AT&T personnel were not allowed to access the site in order to restore power because 1) the building had not been determined to be structurally safe enough to enter, and 2) the area was being assessed as a crime scene.

In the report, AT&T committed to improving its network resiliency, communications with 911 centers, and its backup-power capabilities. AT&T action items in response to this incident include:

- Evaluating engineering electrical-power-shutoff infrastructure nationwide.
- Conducting engineering studies to enhance backup-generator flexibility and capability.
- Talking with government officials about establishing national protocols to expedite access.
- Diversifying the communications paths to 911.

(Source: IWCE's Urgent Communications)

FEMA updates 25 Incident Management Team Job Title/Position Qualifications and Position Task Books

FEMA's National Integration Center (NIC) has updated the Job Titles / Position Qualifications and National Qualification System (NQS) Position Task Books (PTBs) for 25 Incident Management Team (IMT) positions.

The update is a product of stakeholder input as part of periodic reviews conducted by the NIC. These documents were last updated in 2017.

This update is a substantial one, including the Incident Commander, all of the Incident Command Staff, all Section Chiefs in three of the functional areas of incident management in the Incident Organizational Structure (Planning, Logistics and Finance/Administration), 12 Unit Leaders, three Branch Directors in the Operations Section (Service, Support, and Air Operations) and two Group Supervisors (Air Support and Air Tactical).

The NIC's Position Qualifications define the minimum qualifications criteria for personnel serving in defined incident management and support positions. Position Task Books identify the competencies, behaviors, and tasks that personnel should demonstrate to become qualified for a defined incident management and support position. Together, these documents help to establish resource typing definitions, providing a common language for the mobilization of resources and a common incident management platform for emergency responders and officials.

Visit FEMA's website to review the Position Qualifications and Position Task Books for all 25 updated positions. These updates will also be available to search and browse in the NIC's Resource Typing Library Tool.

(Source: FEMA's National Integration Center)

Webinar: Talking TIM - Unmanned Aerial Systems (UAS) for Traffic Incident Management

The Talking TIM webinar series, brought to you by the Federal Highway Administration (FHWA), provides a forum where Traffic Incident Management (TIM) champions with any level of experience can exchange information about current practices, programs and technologies. Each month, the FHWA TIM Program Team will feature content that highlights successful programs, identifies best practices and showcases technology that advances the profession.

The June 2021 Talking TIM webinar will focus on Unmanned Aerial Systems (UAS) for Traffic Incident Management. Unmanned aerial systems are an emerging technology that is poised to take traffic incident management (TIM) to a new level of speed, precision and efficiency. UAS reduces responder time on scene, accelerates crash investigations, creates better situational awareness for responders, and is a cost-effective measuring and mapping alternative.

The target audience for this webinar includes members of transportation agencies, traffic/transportation management center personnel, GIS and mapping staff, traffic data analysts, emergency management organizations and public safety agencies.

Interested participants may obtain 1.5 Professional Development Hours (PDHs) by attending this webinar.

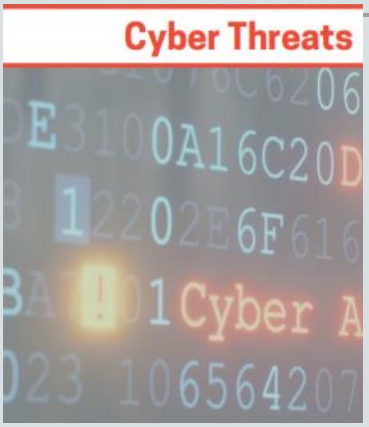
The Talking TIM webinar series is hosted by the National Operations Center of Excellence (NOCoE), a partnership of the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the Intelligent Transportation Society of America (ITSA) with support from the Federal Highway Administration (FHWA).

This free webinar will take place on **June 23, 2021 from 1:30 p.m. to 3:30 p.m. EST**. For more information about the webinar topic, speakers, and how to register, visit the NOCoE's web page for this event.

To learn how you can obtain PDH credits, visit the National Operations Center of Excellence's (NOCoE) Webinar PDH Credits page. You can also visit NOCoE's Talking TIM Webinar Series to access recordings of past webinars and announcements of future webinars in the Talking TIM series.

For more information about TIM technologies, training and data, visit the FHWA Every Day Counts Next Generation TIM initiative.

(Sources: NOCCoE, FHWA)



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

Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists Darkside

The Department of Justice (DOJ) announced on Monday, June 7, 2021, that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation.

On or about May 7, Colonial Pipeline was the victim of a highly publicized ransomware attack resulting in the company taking portions of its infrastructure out of operation. Colonial Pipeline reported to the FBI that its computer network was accessed by an organization named DarkSide and that it had received and paid a ransom demand for approximately 75 bitcoins.

This bitcoin represents proceeds traceable to a computer intrusion and property involved in money laundering and may be seized pursuant to criminal and civil forfeiture statutes.

(Source: DOJ)

FBI: REvil cybergang behind the JBS ransomware attack

The Federal Bureau of Investigation has officially stated that the REvil operation, aka Sodinokibi, is behind the ransomware attack targeting JBS, the world's largest meat producer.

Ransomware attacks have intensified over the past month as threat actors targeted critical infrastructure and services.

TLP Information

The REvil ransomware operation is believed to be operated by a core group of Russian threat actors who recruit affiliates, or partners, who breach corporate networks, steal their data and encrypt their devices. This operation is run as a ransomware-as-a-service, where the core team earns 20-30 percent of all ransom payments, while the rest goes to their affiliates.

REvil, also known as Sodinokibi, launched its operation in April 2019 and is believed to be an offshoot or rebranding of the notorious GandCrab ransomware gang, which closed shop in June 2019.

(Source: BleepingComputer)

Alleged REvil ransomware operator says all US entities can now be targeted

A notorious ransomware gang says it's no longer trying to avoid targets that are based in the United States, and despite the heightened focus from lawmakers, the group says it's doubling its focus on U.S. targets.

In a short interview posted to the Russian OSINT Telegram channel that has since been deleted, an alleged representative of the REvil ransomware gang said the group was behind the attack on global food processing company JBS, but expected the damage to be contained to Brazil, since the company's headquarters is based in São Paulo. The spokesperson said it had tried to avoid U.S. companies at large since the Colonial Pipeline ransomware incident.

Since the Colonial Pipeline hack, the U.S. government has been intensely focused on fighting ransomware. According to a Reuters report, the U.S. Department of Justice will start elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals.

(Source: Intel 471)

CISA: Unpatched VMware vCenter software

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of the likelihood that cyber threat actors are attempting to exploit CVE-2021-21985, a remote code execution vulnerability in VMware vCenter Server and VMware Cloud Foundation. Although patches were made available on May 25, 2021, unpatched systems remain an attractive target and attackers can exploit this vulnerability to take control of an unpatched system.

CISA encourages users and administrators to review VMware's VMSA-2021-010, blogpost, and FAQ for more information about the vulnerability and apply the necessary updates as soon as possible, even if out-of-cycle work is

required. If an organization cannot immediately apply the updates, then apply the workarounds in the interim.

(Source: CISA National Cyber Awareness System)

NYC Law Department system still down three days after hack uncovered

The New York City Law Department's computer system remained down on Tuesday, June 6, about three days after investigators discovered the agency had been hacked. The FBI and members of the city's Cyber Command office are doing a forensic analysis of the incident and trying to figure out a motive for the attack, which was first reported by the Daily News. The hackers have yet to demand a ransom, but a top New York Police Department (NYPD) official didn't rule out the possibility down the road.

(Source: New York Daily News)

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