SAFECOM &
NATIONAL COUNCIL OF STATEWIDE
INTEROPERABILITY COORDINATORS
(NCSWIC)

FALL 2023 MEETING

Cape Coral, FL | December 4-7, 2023

Fall 2023 Joint SAFECOM-National Council of Statewide Interoperability Coordinators Bi-Annual Meeting

Executive Summary | December 6, 2023

The Westin Cape Coral | Cape Coral, Florida

Contents

Welcome and Opening Remarks

Chief Gerald Reardon, SAFECOM Chair, Brad Stoddard, National Council of Statewide Interoperability Coordinators (NCSWIC) Chair, and Billy Bob Brown, Jr., Cybersecurity and Infrastructure Security Agency (CISA) Executive Assistant Director (EAD) for Emergency Communications, welcomed members to the joint meeting in Cape Coral, Florida.

Chief Reardon commended attendance levels as this was one of the largest turnouts of both SAFECOM and NCSWIC members in a long time and expressed his gratitude for those traveling between holidays. He emphasized the value of in-person meetings, noting how bringing together this concentration of knowledge and experiences contributes to an exchange of best practices and lessons learned across the community. Mr. Stoddard shared his gratitude for CISA's support. He noted NCSWIC met individually the day before, emphasizing the importance of building relationships.

EAD Brown introduced Mr. Jay Gamble, CISA Region 4 Regional Director, who discussed how CISA's regional model mirrors the Federal Emergency Management Agency (FEMA) regional model. CISA has a host of emergency communications and cybersecurity professionals working together who are available to assist state, local, tribal, and territorial public safety communications organizations. EAD Brown concluded by noting this level of collective brain power is what it takes to solve the public safety communications community's biggest challenges.

Keynote: CISA's Deputy Director on Public Safety Communications

CISA Deputy Director Nitin Natarajan addressed the agency's strategic focus areas and plans to work with public safety to address communications interoperability and cybersecurity issues now and into the future. He emphasized CISA's commitment to both the

SAFECOM and NCSWIC programs and provided insight into cross-over priority areas being driven by CISA and affecting the public safety communications community:

- CISA will continue to dedicate significant resources toward existing and emerging threats, especially those related to artificial intelligence (AI) and machine learning, as both technologies represent powerful tools and significant risks now and into the future.
- CISA continues to focus on physical and cybersecurity threats, emphasizing how they relate to emergency communications for this community.
- CISA wants to learn more about the public safety community's greatest challenges and priorities to help identify and dedicate necessary assets toward boots-on-the-ground efforts and preventative and resiliency measures for all levels of government; this becomes more important over time as CISA has been receiving an increasing number of requests for assistance; quantifiable justifications are key to securing resources, as the Hill seeks measurable evidence for return on investment, which is a challenge when it comes to calculating the success of prevention.
- CISA is working more broadly to incorporate global best practices, including public safety standards from different countries.
- CISA and public safety should be working together to cultivate the next generation workforce; shifts in required skillsets for those working in emergency communications are at a crucial juncture; there needs to be a better understanding of the talent needed to replace, expand, and elevate an aging workforce.
- CISA and the public safety community should work more closely to combat increasing threats to critical sectors and facilities, such as hospitals and 911 centers; the adversarial pool and frequency of targets will only grow requiring comparable countermeasures.
- CISA continues to bring together Emergency Communications Coordinators (ECCs) with Cybersecurity Advisors (CSAs) and develop rapid cyber assessments for land mobile radio (LMR).

Photo: CISA Deputy Director Nitin Natarajan addressing SAFECOM and NCSWIC

Photo: SAFECOM and NCSWIC members assembled for the Fall 2023 SAFECOM-NCSWIC Bi-Annual Meeting

Response to Real World Events: Maui Wildfires

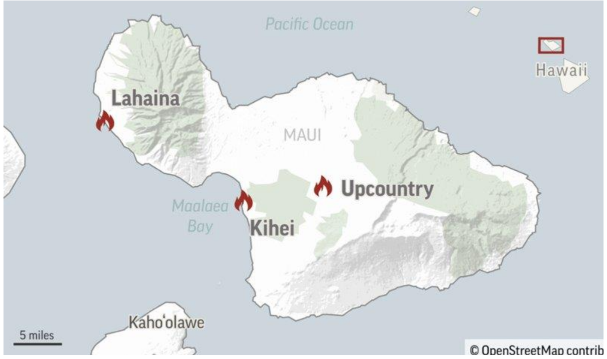

Figure 1: Map of Maui Wildfires, August 2023

Tom Lawless, CISA Region 9 ECC, shared his experiences as a responder to the August 2023 Maui wildfires and detailed challenges, best practices, and lessons learned. First, Mr. Lawless discussed preceding events that exacerbated the fire, including a decade-long drought, widespread growth of easily burned invasive grasses, and depleted resources due to Hurricane Dora response. He also explained that the hurricane's winds prevented dedicated firefighting aircraft from deploying once the fire began and knocked down utility poles, which later blocked fire evacuation routes. Mr. Lawless additionally noted that only 60 to 70 firefighters are on duty on the entire island at any one time, and at the time of the August fires, they were simultaneously fighting four fires at once. Mr. Lawless detailed that both students and instructors from a recent Incident Command System (ICS) course led on Kauai were deployed to Maui to respond, pointing to the value of training and exercising prior to response.

Next, Mr. Lawless reviewed the fire timeline, which began August 7. Another small fire began in Lahaina in the morning of August 8 and, while it was declared contained after several hours, a second fire started that afternoon as well. This fire burned Lahaina's downtown, blocked roads, and disrupted cellular service within three hours. Occupants were forced to flee to the ocean for safety and assistance.

Although Lahaina lost cellular service by August 8, the public safety radio system remained online; however, the fire destroyed fiber optic backhaul that connects the communication offices in Lahaina. The Maui Communications Chief (MCC) ordered mobile, temporary towers from AT&T, Verizon, and T-Mobile as well as Starlink Internet Terminals to assist shelters and recovery centers. Originally, the MCC did not request external support, but after one week, he submitted a request for Mr. Lawless' on-site help. Mr. Lawless detailed how he assisted MCC staff, including working with them to clearly identify roles needed to organize and prioritize communications. The team created a dedicated email inbox, identified a landline telephone designated for the help desk, and established a Maui Communications Task Force Adobe Connect room to streamline communications efforts and reporting.

Finally, Mr. Lawless reviewed takeaways and lessons learned, including the importance of providing first responders with emotional, mental, and physical support and of utilizing Telecommuter Emergency Response Taskforces to support operations in environments where the victims are also the responders. Mr. Lawless encouraged attendees to manage recovery timeline expectations, maintain cultural sensitivity, and deploy less-utilized technologies, such as Civil Air Patrol and drone operations, General Motors' OnStar Disaster Service, and Pacific Disaster Center's DisasterAware Pro during response.

Link Layer Encryption and Link Layer Authentication

Mr. Scott Wright, SAFECOM At-Large, State of Connecticut Department of Emergency Services and Public Protection and Connecticut Co-Statewide Interoperability Coordinator (SWIC), Ms. Hermina (Nina) Koshinski, SAFECOM At-Large, Chief of Radio Operations Engineering & Support, Statewide Radio Network Division, Pennsylvania State Police, and Mr. Justin Evans, Radio Systems Manager, Montgomery County Hospital District, spoke to the latest updates with link layer encryption (LLE) and how LLE differs from link layer authentication (LLA). Discussions addressed why agencies should employ the use of these features (LLE when available) as well as challenges with cybersecurity.

The group discussed in detail the difference between LLA and LLE. The LLE Project 25 (P25) standard is still under development. Ms. Koshinski discussed how LLA works in a P25 trunked system and the benefits for public safety users. LLA gives system administrators and planners a useful cyber security tool for combating unauthorized access to their P25 trunked systems, which can occur if a threat actor gains access to a cloned or spoofed subscriber unit ID (SUID). As the capabilities and tools to eavesdrop, monitor, steal, or disrupt public safety communications become easier to acquire, additional security measures such as LLA are needed to protect unauthorized access to public safety communications systems. The panelists stressed this security service is well worth the effort to implement for the increased security. They also discussed challenges with LLA, including implementing the security service with

InterRadio Frequency (RF) Subsystem Interface (ISSI). Ms. Koshinski and Mr. Evans presented brief use cases on the resolutions their agencies implemented.

Mr. Evans emphasized this is a fluid process. Joint SAFECOM-NCSWIC P25 User Needs Working Group (UNWG) members work closely with manufacturers to ensure that the developed standards are able to be implemented. UNWG members actively participate in multiple calls each month to represent the user community and address how these standards will impact the community. He noted as passionate users, they are concerned about their infrastructure and network security and have chosen to actively engage in this process, rather than passively waiting for manufacturers to define standards; instead, UNWG members are actively collaborating with manufacturers, a crucial aspect in this process. While the timeline remains uncertain, the Working Group's ultimate goal is to develop a standard that meets our needs and is interoperable on our networks. This exemplifies the significance of UNWG's existence and its vital role in the standards process.

Questions and comments from the audience included interest in LLE and how it would work when implemented; how to implement LLA in an existing system; how the security service works with disparate systems; and advice on implementation of LLA in new systems. Mr. Evans, Mr. Wright, and Ms. Koshinski answered these questions and advised the audience to read, *LLA and LLE: Are you Really Secure?*, a white paper written by the UNWG, available on the SAFECOM website.

Next Generation 911

Mr. Mel Maier, CEO/Executive Director, Association of Public Safety Officials - International (APCO), provided an overview of the Public Safety Next Generation 911 (NG911) Coalition and the successful efforts by public safety to define NG911 and interoperability to ensure we share the same fundamental understanding of what NG911 is. Mr. Maier highlighted the benefits of NG911 to enhance the interoperability and security of 911 systems. He shared available resources, such as APCO's *Sample Request for Proposal Template for NG911 Capabilities* and APCO's Definitive Guide to Next Generation 911. NG911 is more than just new inputs into the 911 center; it's about improving the safety of the caller, providing essential scene safety information to the field-based responders, and dispatching the most appropriate resources as quickly as possible. NG911 will be saving lives in our communities the moment it is deployed.

Mr. Budge Currier, 911 Administrator, California Governor's Office of Emergency Services, provided updates on the deployment of NG911 across the State of California's 449 Public Safety Answering Points (PSAPs). Mr. Currier shared that 19 PSAPs are actively receiving NG911 calls, while all PSAPs are receiving text-to-911 through California's NG911 Core Services solution. Mr. Currier highlighted the benefits of NG911 and reducing service disruptions; California has not experienced any outages with their NG911 system since implementation. Mr. Currier also discussed how California is testing their Computer-Aided-Dispatch (CAD)-to-CAD data sharing system across 6 different PSAPs to address interoperability challenges and enable data sharing across PSAPs. He also highlighted NG911 Interoperability Task Force initiatives to ensure interoperability across all NG911 systems.

Following the presentation, attendees inquired about funding for California's statewide NG911 system. Mr. Currier shared that California's system is funded through 911 fees. He noted additional costs related to infrastructure and testing. Attendees also inquired how 911 centers are addressing human factors related to receiving multimedia. Mr. Maier and Mr. Currier emphasized the importance of developing policies, procedures, resources, and training to ensure the right individuals receive the right data.

Working Session: Emerging Technology in LMR and the Future of LMR

Chief Reardon and Mr. Stoddard addressed the future of LMR, including broadband-, long-term evolution (LTE)-, and FirstNet-compatible technologies. Participants then broke into working groups for small group discussion on the following topics: architecture issues, LMR-to-LTE solutions, security concerns (e.g., cloud-based technologies interacting with LMR), and the differences between metro and rural areas being able to adopt emerging LMR technologies. Each table brainstormed opportunities and challenges related to the topics.

Participants proposed additional educational opportunities on Mission Critical Push to Talk capabilities and the potential interoperability challenges with proprietary solutions. Participants emphasized the need for funding to procure new LTE technologies and security enhancements to LMR. Additionally, members proposed conversations with manufacturers to ensure LMR standards address user concerns.

Response to Real World Events: East Palestine, Ohio Train Derailment

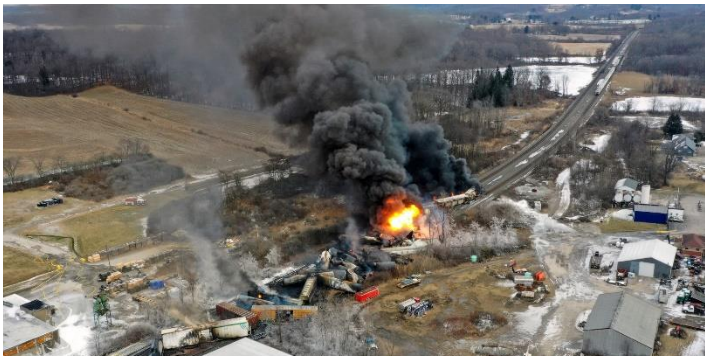

Figure 2: Areal view of the East Palestine, Ohio train derailment, involving 149 train cars--38 of which derailed--with 11 tank cars igniting containing hazardous materials.

A freight train carrying hazardous chemicals derailed and exploded in the town of East Palestine, Ohio, February 3, 2023. The derailment caused the contents of many of the rail cars to spill and an explosion to take place, resulting in a one-mile radius mandatory evacuation. Ohio's statewide radio system, Multi-Agency Radio Communication System (MARCS) deployed a team to support. In this session Mr. Dick Miller, MARCS Field Operations Manager and Communications Unit Leader (COML), and Chief Jamison Conley, Gustavus Township Ohio Fire Department, spoke to how public safety communications in Ohio and surrounding areas were affected during the incident.

Chief Conley, who deployed under the Ohio Fire Chief Plan and supported development of the incident communications plan requirements, described the initial response to the derailment. One day after the incident, the Ohio State Fire Chief's Association was contacted by the Trumbull County 911 Center requesting eight county fire chiefs respond to the staging area in East Palestine. After arriving on scene, one of the fire chiefs requested Ohio MARCS establish a Tower on Wheels (TOW) as well as provide portable P25 cache radios. The Trumbull County Fire Chiefs applied the National Incident Management System (NIMS) ICS model to the response efforts and established command assignments, including planning, logistics, communications lead, staging area manager, and emergency medical services (EMS) staffing. Also requested was an Incident Management Team (IMT) from Butler County, Ohio. Mr. Miller and a MARCS field technician arrived on-scene within roughly two hours of being called, bringing with them the TOW and cache radios. Mr. Miller reported the biggest takeaway from the incident was to get the command structure established early.

Mr. Miller reported on the field operations at the scene. He described the MARCS statewide system, which includes 3,000+ agencies, 150,000+ radios, 74 Sheriff's offices, and 1.8 million average push-to-talks a day. Local communications on-scene consisted of 21 VHF repeaters, including nine for law enforcement, seven for fire, four for EMS, and one for the Emergency Management Agency (EMA). MARCS was requested on Saturday afternoon and was operational within hours. On Sunday, MARCS was cleared to go home approximately two days following the original incident. MARCS was requested to return on Monday morning to supplement the current equipment with an additional TOW and radios to meet the demand of additional agencies coming into the scene and the planning for a controlled explosion. In response to participants' questions, Mr. Miller reported on the railroad company's manifest, which they still have not received. Monitors were set up one to two miles away from the incident for soil and water testing, with 16 to 18 feet of dirt removed from the area around the track to clean out contamination. Mr. Miller reported they did not send out an Integrated Public Alert & Warning System (IPAWS) alert. With regard to the use of data across agencies, Information Technology Service Unit Leaders (ITSL) were not approved for use, resulting in responders using different manufactures and vendors. FEMA did provide data services for federal agencies on Environmental Protection Agency (EPA) activities, but data services were not otherwise leveraged.

National Emergency Communications Plan Update

Ms. Mary Anne McKown, CISA Support, provided updates on the next iteration of the National Emergency Communications Plan (NECP). The NECP team has so far completed the Research and Analysis Phase, which included collaborating with SAFECOM and NCSWIC committees, collecting 175 unique open-source resources, validating findings through working sessions, conducting focus group and integrated IT meetings, and clarifying multifaceted issues related to human factors resilience, encryption, emerging technology, and cyber. The Development Phase will be the next phase executed, which extends from November 2023 to June 2024, and will host stakeholder discussions, identify success indicators for each goal, and develop a draft of the new plan. The final Review and Approval Phase will start in October 2024 and be completed in January 2025. This final phase will include the national engagement period, an adjudication of edits, and a final review and endorsement of the NECP. If anyone is interested in joining the NECP working group, please contact NECP@cisa.dhs.gov. Ms. McKown thanked members for their recent support of the SAFECOM Nationwide Survey (SNS) and noted the data is currently being validated.

Artificial Intelligence

Major George Perera, Miami-Dade Police Department, Major County Sheriffs of America, provided an overview of Open AI tools, such as Chat GPT and DALL-E2, and implications for public safety and cybersecurity. It is increasingly becoming harder for law enforcement to identify artificial images and videos, also known as “deepfakes,” as AI technology advances. He highlighted potential uses of AI by cybercriminals, such as deepfake identification fraud, phishing, and malware attacks. He shared several examples, including an individual changing surveillance camera footage to help exonerate a criminal.

Major Perera also highlighted how AI can be used by public safety and law enforcement to enhance decision making and counter criminal use. AI predictive modeling can be used by law enforcement to provide actionable information to first responders to increase their ability to make decisions based on enhanced information. The Stanford’s Institute for Human-Centered AI developed an AI engine to identify fraudulent videos. In closing, Major Perera noted challenges with prosecuting certain cases as legislation does not address these rapidly-evolving technologies.

Coordinating with CISA

In this session, CISA representatives provided guidance about CISA’s latest resources, offerings, and services. They also provided a preview of the federal resource fair to obtain information about CISA’s latest offerings and services direct from program representatives. Mr. Michael Rits, CISA, shared the new Nationwide Interoperability Services (NIS) organization chart and identified the new branches.

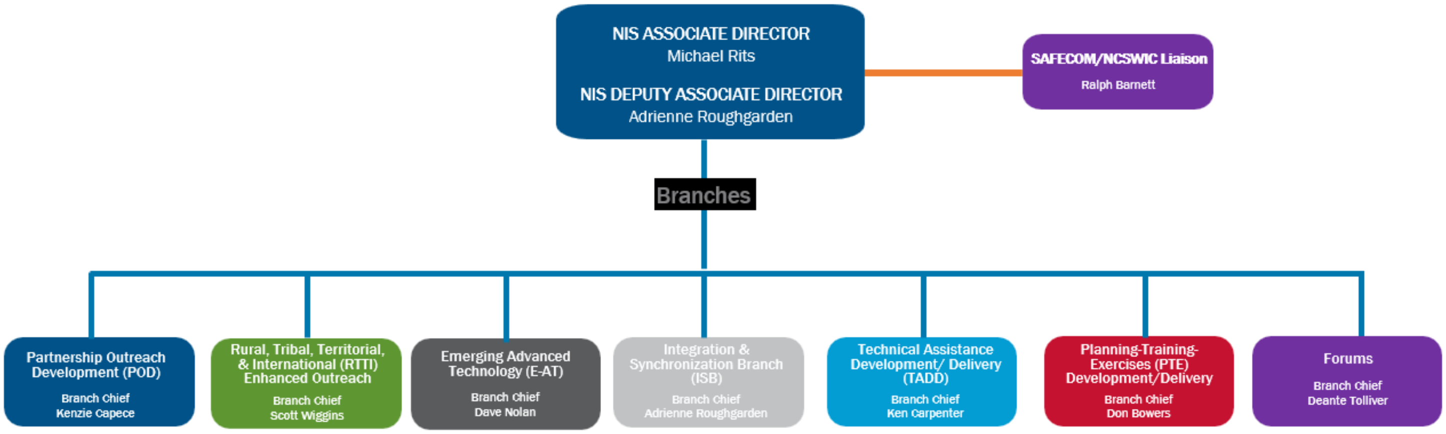
NIS ASSOCIATE DIRECTOR
Michael Rits
NIS DEPUTY ASSOCIATE DIRECTOR
Adrienne Roughgarden
SAFECOM/NCSWIC Liaison
Ralph Barnett
Branches
Partnership Outreach Development (POD)
Branch Chief
Kenzie Capece
Rural, Tribal, Territorial, & International (RTTI) Enhanced Outreach
Branch Chief
Scott Wiggins
Emerging Advanced Technology (E-AT)
Branch Chief
Dave Nolan
Integration & Synchronization Branch (ISB)
Branch Chief
Adrienne Roughgarden
Technical Assistance Development/ Delivery (TADD)
Branch Chief
Ken Carpenter
Planning-Training-Exercises (PTE) Development/Delivery
Branch Chief
Don Bowers
Forums
Branch Chief
Deante Tolliver

Figure 3: CISA ECD NIS Organizational Structure

CISA representatives, Mr. Don Bowers, Mr. Chris Essid, and Mr. Lew Morrison, reported updates to the existing opportunities for members to utilize CISA’s resources, such as the new technical assistance offerings.

Ms. Aislinn Foltz-Colhour, CISA Support, discussed pivotal CISA ECD Grants Policy Branch resources and programs. In particular, she reviewed details about the *SAFECOM Guidance on Emergency Communications Grants*, which is an annually-updated resource that provides current information on national policies, eligible costs, best practices, and technical standards for state, local, tribal, and territorial grant recipients investing federal funds in emergency communications projects; the List of Federal Financial Assistance Programs Funding Emergency Communications, identifies federal financial assistance opportunities (i.e., grants, loans, cooperative agreements) that support emergency communications investments; and the Rural Emergency Medical Communications Demonstration Project (REMCDP) cooperative agreement.

Ms. Laura Goudreau, CISA, announced that the division is currently exploring opportunities to develop games as it pertains to emergency management and planning. She and Mr. Robert Hugi, CISA, participated in recent gaming conferences on behalf of the agency to learn the innovative ways games have been evolving to improve strategic planning skills among public safety officials.