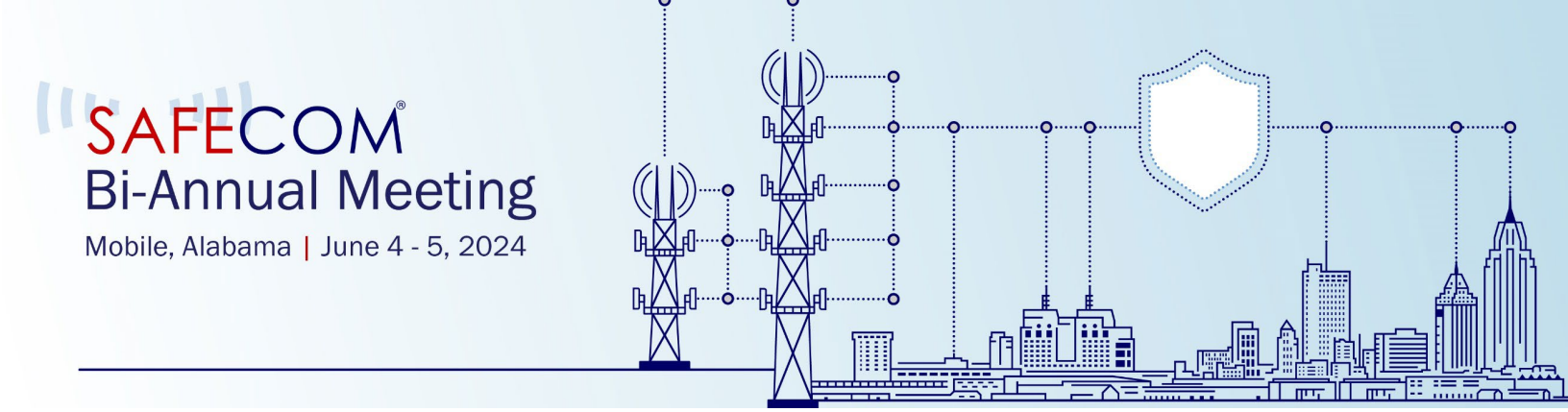

Spring 2024 SAFECOM Bi-Annual Meeting

Executive Summary | June 4, 2024

The Battle House Renaissance Hotel Mobile | Mobile, Alabama

Contents

Welcome and Opening Remarks

Speakers: Chief Gerald Reardon, *SAFECOM Chair*
Assistant Chief Chris Lombard, *SAFECOM First Vice Chair*
Chief Jay Kopstein, *SAFECOM Second Vice Chair*
Vince DeLaurentis, *Cybersecurity and Infrastructure Security Agency (CISA) Deputy Executive Assistant Director (D/EAD) for Emergency Communications*

Session Description: SAFECOM members were welcomed to Mobile, Alabama, for the Spring 2024 SAFECOM Bi-Annual Meeting. Members received opening remarks from SAFECOM and CISA Emergency Communications Division (ECD) Leadership.

Key Outcomes:

- Chief Reardon encouraged SAFECOM to continue pressing forward in the advances that are being made in the public safety communications space while also embracing new technology and molding it to fit public safety interest.
- D/EAD DeLaurentis welcomed SAFECOM members and acknowledged the hard work being done by SAFECOM across the nation on bolstering emergency communications and highlighted the recent success of Emergency Communications Month, the Alerts Warnings and Notifications Meeting, and the World Cup Planning Workshop.

- Technical assistance (TA) and Statewide Communications Interoperability Plans (SCIP) were also mentioned as top priorities for CISA. CISA is working on improving the process in which TA and SCIPs are administered by soliciting feedback/comments from SAFECOM.

Action Item: Members with suggestions on how to improve TA and SCIP administration should contact SAFECOMGovernance@cisa.dhs.gov

Artificial Intelligence

Speakers: Major George Perera, *Major County Sheriffs of America (MCSA), Miami-Dade Police Department (Florida)*
Dr. Syed Mohammad, *Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Director for Modeling and Simulation Engine*
Mr. Amidu Kamara, *DHS S&T*

Session Description: Panelists provided updates about ongoing developments in Artificial Intelligence (AI), including threats and ways to leverage AI for communications missions.

Key Outcomes:

- Phishing attacks using AI have increased over 300%. Cybercrime accounts for over $8.5 trillion a year making it the third largest economy behind the United States and China.
- Cybercrime is entering a poly-criminal age where transnational criminal organizations are engaging in cybercrime.
- DHS S&T are using AI predictive threat modeling to assist public safety agencies (e.g., United States Coast Guard and United States Border Patrol) in creating an AI modeling solution to leverage historical data and allow public safety agencies to be proactive in suspicious behaviors, patterns, and dependencies.
- DHS S&T is advancing research in AI to improve machine learning models through first principle models, manage uncertainty, address AI risks, and enhance explainable AI for more reliable and effective communication mission.

SAFECOM Member Spotlight: International Association of Certified Information Sharing and Analysis Organizations

Speakers: Ms. Deborah Kobza, *International Association of Certified Information Sharing and Analysis Organizations (IACI) Chief Executive Officer*
Mr. Todd Hillis, *IACI Chief Information Officer*

Session Description: Panelists from one of SAFECOM's newest associations, IACI, briefed on their current public safety communications priorities and products.

Key Outcomes:

- The mission of IACI is to provide resources and collaborative opportunities focused on security convergence and information sharing.
- IACI has a library of 24/7 real time "actionable" intelligence, such as the IACINet Malware Information Sharing Platform, available to the public and private sector to build system resilience and combat malicious activities.

NEW MEMBER INTRODUCTIONS

SAFECOM Chair, Chief Gerald Reardon, introduced and welcomed new SAFECOM members:

- Matt Butler, International Association of Certified ISAOs (IACI) [Primary]
- Laura Cooper, Major Cities Chiefs Association (MCCA) [Primary]
- Brent Finster, At-Large, Douglas County Dept of Emergency Management
- Trevin Hunter, At-Large, Louisville Metro Emergency Services
- Deborah Kobza, IACI [Alternate]
- Robert Ricker, At-Large, Alsip Fire Department

Chief Reardon also acknowledged former SAFECOM members who have departed since the last meeting:

- Cindy Cast, At-Large, Miami-Dade County
- Jesse Cooper, MCCA [Primary]
- Nicole Diedrick, At-Large, Phoenix Police Department – Communications Bureau

FirstNet Authority Update

Speaker: Ms. Jacque Miller-Waring, *Area Director, Public Safety Engagement, FirstNet Authority*

Session Description: Members received an update from the FirstNet Authority on current initiatives, including additional geographical coverage in rural areas, continued collaboration on a framework for broadband talk group naming, and system performance notification processes.

Key Outcomes:

- The FirstNet Authority shared success stories and information about network investments to expand the FirstNet Deployables fleet, enhance the FirstNet Core for Fifth Generation (5G) network capabilities, improve in-building coverage and resiliency, and continue network evolution.
- The FirstNet Authority's Mutual Aid Framework Project facilitates the development of a mutual aid framework for broadband Mission-Critical Push-to-Talk (MCPTT) that addresses talk group organization and governance nationwide and will ensure first responders can communicate efficiently and effectively when jointly responding to an event; SAFECOM, together with the FirstNet Authority, is reestablishing the MCPTT Working Group and solicited SAFECOM participation.
- In response to questions about the recent AT&T system outage, Ms. Miller-Waring shared that the FirstNet Authority is working to improve notification policies and procedures so public safety stakeholders can make informed decisions.
- Attendees encouraged the FirstNet Authority to push vendors to harden sites and increase power capabilities, as emergency communications systems are increasingly reliant on the broadband network; the FirstNet Authority plans to have conversations with critical infrastructure at the state and local level.

Figure 1: SAFECOM Members, June 2024

Action Item: SAFECOM members interested in joining the MCPTT Working Group should email SAFECOMGovernance@cisa.dhs.gov

PACE Planning Briefing

Speakers: Mr. Charlie Guddemi, *District of Columbia Statewide Interoperability Coordinator (SWIC)*
Mr. Brandon Smith, *CISA Emergency Communications Coordinators Western Sector Coordinator*

Session Description: Panelists discussed the ways in which Primary, Alternate, Contingency, Emergency (PACE) planning can reduce and diversify risk. Members participated in a group discussion about PACE planning.

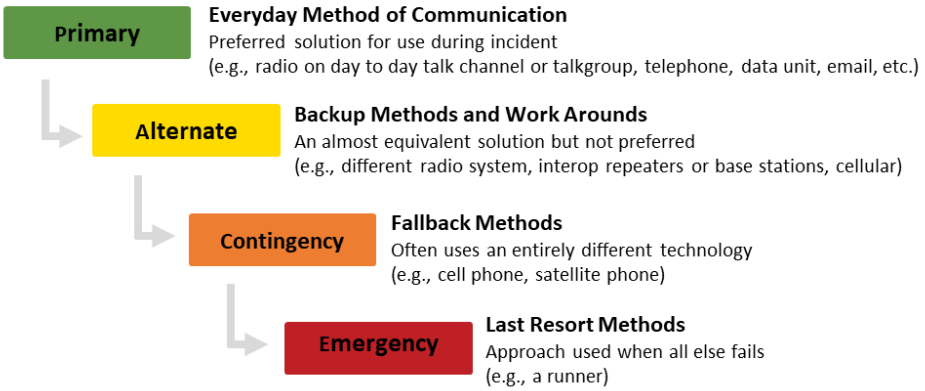

Figure 2: PACE: Primary, Alternate, Contingency, Emergency Planning

Key Outcomes:

- Speakers emphasized the importance of having a diverse PACE Plan, and to not use "all-in-one" solutions which are really anti-PACE and can fail during a response to a man-made or naturally caused emergency. Agencies should practice their PACE plan often and agency personnel should be well familiarized with it.
- Panelists highlighted the difference between tools and solutions; for example, utilizing Long-Term Evolution (LTE) and Land Mobile Radio (LMR) are tools for communication, but not a solution or plan for communication.
- Mr. Smith discussed the response needed for a presidential inauguration to show the value in evaluating both physical and cyber vulnerabilities as both can have detrimental effects; an event can have a strong physical security presence and still be taken down by a cyberattack.
- While technology and new products are emerging at a rapid rate, Mr. Guddemi emphasized the value of including, and providing training for, past technologies and protocols (e.g., runners as communicators) as part of the "Emergency" aspect of the PACE plan because it would mean that the Primary, Alternate, and Contingency plans have already failed.

Next Generation 911 Updates Across the Country

Speaker: Mr. Adam Wasserman, *National Association of State 911 Administrators (NASNA)*

Session Description: Members received an overview of where states are in their progress toward implementing Next Generation 911 (NG911). As the nation progresses towards NG911, all states are moving towards NG911 and are in various stages of their NG911 transition. The session included a synopsis of the phases of NG911 and where states are in that journey. The session also covered some of the obstacles that states face in NG911 progress and their experiences with NG911 success.

Key Outcomes:

- Mr. Wasserman discussed the benefits of NG911 to enhance the reliability and resiliency of 911 systems, such as diversifying call delivery to allow Emergency Communications Centers (ECCs) to easily route and transfer calls.
- Mr. Wasserman reviewed the transition challenges to NG911, such as funding, governance, and planning.
- Attendees emphasized the importance of planning for and designating alternate call routes with NG911. ECCs will have the ability to route calls to an alternate ECC in the event of an outage or an incident where the ECC is overwhelmed with calls. It will be critical for ECCs to develop policies and procedures to ensure that the appropriate information is shared with local first responders.
- Members discussed challenges with routing calls from the National 988 Suicide and Crisis Lifeline, as calls are routed by area code, not by geographic location, to maintain the caller's anonymity. Calls for service are transferred to the local ECC through a 10-digit transfer. NASNA is engaging with the Substance Abuse and Mental Health Administration and service providers to address challenges.

Action Item: Potential future session on CISA Computer-Aided Dispatch (CAD) initiatives

Information Sharing Framework Update

Speaker: Sheriff Paul Fitzgerald, *National Sheriffs' Association (NSA), Information Sharing Framework Task Force Chair*

Session Description: Members received an update from the Information Sharing Framework Task Force (ISFTF).

Key Outcomes:

- The ISFTF continues to work with the Iowa Department of Public Safety applying the Information Sharing Framework (ISF) in assessing vendors in their Request for Proposal (RFP) for interoperability in CAD-to-CAD information sharing within the state; the Department is in the final stages of vendor assessment and a decision should be made soon.
- The RFP will consist of objectives to provide the industry more flexibility in how to plan, design, and test the service platform and the Statement of Work will include all requirements.

- The ISFTF continues to present at events, such as the Interoperability Institute hosted by the Texas A&M University Internet2 Technology Evaluation Center (ITEC), to raise awareness about the Task Force and relevant uses of ISF concepts.

Action Item: Members interested in joining the Task Force or looking to provide operational input should reach out to Sheriff Paul Fitzgerald, National Sheriff's Association, or Mr. Rob Dew, CISA

Cybersecurity Session

Speaker: Major George Perera, *MCSA, Miami-Dade Police Department (Florida)*

Session Description: Members learned about the Miami-Dade Police Department (MDPD) Cyber Crimes Bureau, including how it was created, what it does, how cybercriminals are tracked and prosecuted, and the trends/growth rates based on collected data.

Key Outcomes:

- The MDPD received thousands of cyber complaints from its citizens with losses equaling up to $750 million in 2023. Partnering with the U.S. Secret Service provided additional federal resources to the MDPD such as the ability to analyze, investigate, and prosecute cybercrimes on the federal level.
- The top 3 cyber complaints in the United States are business email compromise, crypto scams (romance/investment), and ransomware.
- MDPD investigates many types of cybercrimes, including network intrusion, crypto currency, money laundering and cyber fraud, malware, business email compromises, romance scams, and dark web crimes. MDPD is actively working to keep up with intelligence trends, specifically narcotics transactions and internet crimes against children. Deployable units are also available to respond to major crime investigations with the capabilities to pull video, map wireless networks, and get information from wireless access points in the vicinity of the crime.

Encrypted Storage Location Number Assignment Coordination

Speakers: Ms. Hermina "Nina" Koshinski, *Pennsylvania State Police, Statewide Radio Network Division*
Mr. Scott Wright, *State of Connecticut Department of Emergency Services and Public Protection, Connecticut Deputy SWIC*
Mr. David Moore, *National Law Enforcement Communications Center (NLECC)*
Assistant Chief Michael Baltrotsky, *Technology Section Chief/CIO at Montgomery County (MD) Fire & Rescue*
Mr. Wes Rogers, *CISA*

Session Description: Panelists discussed efforts to coordinate assignment of Storage Location Numbers (SLN).

Key Outcomes:

- Ms. Koshinski discussed two critical incidents in 2023 and how communications with federal partners were critical to a successful outcome. Air assets have always been a challenge during major incidents and need to be addressed. Pennsylvania implemented the use of 700-MHz Air-to-Ground frequency channels and an IO encryption key that all partners already had and could use. Ms. Koshinski explained that this bank of frequencies had already been shared with another state and some local organizations. This process could be implemented throughout states in the Northeast region or possibly elsewhere, which would allow federal partners to program in one bank of channels that can be reused with multiple entities.
- The key management facility (KMF) allows for centralized distribution of key material. Transferring keys between Key Fill Devices can unintentionally introduce errors, which can then be compounded.
- Training personnel on the use of encryption allows users to better prepare for issues regarding LMR encryption or know the subject matter expert available to remedy an issue.
- Panelists requested that an appropriate user-led group develop best practices to include passwords and field devices.

Action Items:

- Panelists emphasized the need to use only Advanced Encryption Standard-256 and encouraged members to completely phase out the use of Data Encryption Standard (DES) since it is no longer NIST approved, and its use is depreciated.
- Members will develop a document that discusses why encryption is important and will highlight the lessons learned from cases such as the National Capitol Region.

Federal Communications Commission Update

Speaker: Mr. Roberto Mussenden, *Federal Communications Commission (FCC)*

Session Description: Members received an update from the FCC, including an update on the 4.9 GHz public safety spectrum.

Key Outcomes:

- The Commission shared its newest capability: performing wireless cellular network assessments by collecting, analyzing, and providing reports on spectrum usage for both notice and non-notice events.
- The Commission is planning to finalize an agreement under the new General Coordination Agreement (GCA) for FirstNet's operations along the Canadian border, add air-ground provisions to agreements for 700 MHz and 800 MHz, and look for opportunities to expand the availability of VHF interoperability channels along the border.
- Members were informed about how to avoid public safety licensing issues by providing an agency or title email instead of a personal email. For assistance, Mr. Mussenden shared licensees can contact the FCC ULS support staff but may also contact an FCC public safety coordinator that will be able to update administrative information or renew a license for a fee.
- Members were informed about the latest updates for 4.9 GHz band rulemaking with the goal of maximizing the potential of the spectrum. These updates include establishing a nationwide band manager, a proposal to collect more specific data on public safety deployments in the band, and technical changes to Part 90 rules to allow licensees to deploy the latest commercially available technology, including 5G, in the band.

Action Item: The 4.9 GHz Ninth Further Notice of Proposed Rulemaking seeks comments on specific criteria for protecting public safety licensees operating in the band from harmful interference

Closing Remarks

Speakers: Chief Gerald Reardon, *SAFECOM Chair*
Assistant Chief Chris Lombard, *SAFECOM First Vice Chair*
Chief Jay Kopstein, *SAFECOM Second Vice Chair*

Session Description: SAFECOM Leadership provided closing remarks, to include updates on the Fall 2024 Bi-Annual Meeting and encouraged members to provide feedback on the meeting via a feedback survey.

Key Outcomes:

- Save the date for the Fall 2024 SAFECOM Bi-Annual Meeting: November 18-22, 2024; Location and additional logistics information forthcoming.

Action Item: SAFECOM members were encouraged to participate in the Meeting Feedback Survey as their input in the survey kicks off development for the next bi-annual meeting.

SAFECOM SUB-GROUP MEETINGS

June 5, 2024

In addition to the SAFECOM Bi-Annual Meeting, members of the NG911 Working Group, SAFECOM Governance Committee, and SAFECOM Executive Board met to further collaborate on identified work products. Separate meeting summaries were developed to capture major action items and outcomes from those meetings.