SAFECOM

# FALL 2022 SAFECOM BI-ANNUAL MEETING

Jacksonville, FL | December 13 – 14, 2022

## Executive Summary | Tuesday, December 13, 2022

### Contents



**WELCOME NEW MEMBERS!**

- **Dr. Hezedean Smith:** National EMS Management Association (NEMSMA) (Primary)
- **Charles Blankenship:** NEMSMA (Alternate)

### Welcome Remarks and New Member Introductions

SAFECOM Leadership, including Chief Gerald Reardon, SAFECOM Chair and SAFECOM At-Large, City of Cambridge Fire Department, Massachusetts; Deputy Chief Chris Lombard, SAFECOM First Vice Chair and SAFECOM At-Large, Seattle Fire Department, Washington; and Chief Jay Kopstein, SAFECOM Second Vice Chair and SAFECOM At-Large, New York State Division of Homeland Security and Emergency Management, welcomed members to the Fall 2022 SAFECOM Meeting in Jacksonville, Florida. Chief Reardon congratulated members on another tremendously successful year and highlighted numerous, newly-published resources available on the SAFECOM website. He also emphasized that, while valuable, these resources can only be helpful when implemented at the state, tribal, territorial, regional, and local levels, and encouraged members to continue to share them with their constituents and agencies.

Deputy Executive Assistant Director Vincent DeLaurentis, Cybersecurity and Infrastructure Security Agency (CISA), welcomed participants and added that CISA's partnership with SAFECOM is critical to future success. He encouraged members to participate in the upcoming SAFECOM Nationwide Survey (SNS).

*Photo: SAFECOM Membership, December 2022*

## FALL 2022 SAFECOM BI-ANNUAL MEETING EXECUTIVE SUMMARY

### Keynote: CISA's Deputy Director Nitin Natarajan

*Photo: CISA Deputy Director, Nitin Natarajan*

Deputy Director for CISA, Nitin Natarajan, again gave the keynote address to SAFECOM on its opening day of meetings. Emphazing the significant evolution of communications over the years, Mr. Natarajan spoke to CISA's continual efforts to do substantive work across relevant communities to solve increasing challenges. He stressed the work SAFECOM does to contribute to a stronger and safer nation and CISA's commitment to working with the broader emergency communications community to leverage their expertise. He sought feedback from membership on how to improve the Agency's own communication with SAFECOM. CISA, Mr. Natarajan detailed, continues to improve on its own internal cross-collaboration to ensure divisions are aware of activities and efforts across the whole Agency, including those projects and pieces of guidance being addressed and written by SAFECOM. CISA also wants to ensure relevant information on cybersecurity is reaching its communities, such as its campaigns to launch a "311" national emergency call line and clinic following cyber incidents and to push for compliance using multi-factor authentication nationwide by 2025. Chief Reardon asked how public safety agencies begin coordination with CISA following a cyber event, to which Mr. Natarajan emphasized the need to reach out to the Emergency Communications Coordinator within the affected state. Mr. Natarajan continued to coordinate during and after the day's events with membership and CISA staff in support of SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) meetings that week.

### Surfside Building Collapse: Experiences from the Communications Unit

Cindy Cast, SAFECOM At-Large, Radio System Manager, Miami-Dade County, Florida, and Pam Montanari, CISA Region IV Emergency Communications Coordinator, presented a briefing on the June 24, 2021, building collapse at Champlain Towers South—a 12-story beachfront condominium located in the Miami suburb of Surfside, Florida, resulting in the loss of 93 individuals. Ms. Cast served as the local Communications Coordinator (COMC) for the incident, and Ms. Montanari was deployed in support as well. They shared challenges and successes encountered while delivering emergency communications services and equipment for the response and recovery operations, which continued for 33 days. Public safety agencies were heavily engaged in several key priorities, including:

- Search and rescue
- Triage, treatment, and transportation of the injured
- Firefighting and salvage
- Scene security and safety
- Remains identification and notification of next-of-kin
- Establishment and operation of a family assistance center
- Protection and collection of evidence
- Support for personal needs of responders

*Photo: Response and recovery operations in Surfside, FL*

These activities drove the need for emergency communications capabilities (voice, data, and video) in both secure and clear modes. Some challenges included:

- Mobilization of more than 80+ fire and rescue units (two of which were international), 7 Federal Emergency Management Agency (FEMA), and 8 Florida state Urban Search and Rescue teams because of Local Emergency, State of Emergency, and Federal Disaster Declarations issued within the first 24 hours of the initial response
- Insufficient means to achieve all interoperability requirements, as some teams did not have access to the Advanced Encryption Standard (AES) or had equipment with the wrong encryption keys
- Requirement to provide heavy equipment operators with radios to communicate with spotters, fire and rescue personnel, and criminal investigators

- Disruptions in the search mission caused by firefighting operations, severe weather, and instability of the structure
- Frequency deconfliction, as well as operating and maintaining land mobile radio (LMR) networks and deployed communications assets

Key points contributing to successful incident outcomes, including:

- The National Interoperability Field Operations Guide was invaluable to the procurement of additional spectrum needed to support mission requirements
- Strong, well-established, professional relationships between Ms. Cast and federal officials with CISA, the Federal Aviation Administration, and the Federal Communications Commission (FCC) assured rapid response to unmet needs, access to critical communications and supply resources, and safer and better supported strategic and tactical operations at the scene

### SAFECOM Member Spotlight: Forestry Conservation Communications Association

Lloyd Mitchell provided a SAFECOM Member Spotlight presentation on the Forestry Conservation Communications Association (FCCA). FCCA was established after World War II when first responders began using two-way radios to fight wildfires. Initially serving forestry conservation, the organization has since expanded to support local government radio services. Mr. Mitchell provided an overview of FCCA's primary functions, including radio operations assistance for federal, state, and local governments; suitable frequency identification; FCC licensing assignment recommendations; and frequency protection. He focused on relevant sections of 47 Code of Federal Regulations (CFR) Part 90 – Private LMR Services, specifically highlighting Public Safety Radio Pool (Subpart B) and Policies Governing the Assignment of Frequencies Today (Subpart H). FCCA serves all public safety licensees and maintains partnerships with SAFECOM, the National Wireless Communications Council, and the National Public Safety Telecommunications Council.

### FCC Regulatory Update

Roberto Mussenden, FCC, provided a regulatory update on FCC Public Safety and Homeland Security Bureau actions involving spectrum issues, alerting, 911, resiliency, and disaster response and recovery. After almost 17 years, the FCC terminated the 800 MHz rebranding proceeding. It also vacated the Sixth Report and Order that would have authorized statewide licensees to lease 4.9 GHz spectrum within their jurisdictions. The FCC issued the Eighth Further Notice of Proposed Rulemaking (NPRM) that proposes a nationwide framework for the 4.9 GHz band and emphasizes public safety needs. The FCC sought public comment on ways to foster greater public safety use of the band; and ways to facilitate non-public safety access to the 4.9 GHz band that is compatible with public safety. Additional updates included:

- **Priority Services:** Adopted a Report and Order that updates priority services (May 2022)
- **Network Resiliency:** Released a Report and Order and Further NPRM to adopt the Mandatory Disaster Response Initiative to allow service providers to enter reasonable arrangements for roaming during disasters and establish arrangements for providing mutual aid during disasters (July 2022)
- **Outage Information Sharing:** Implemented rules allowing federal, state, and territorial agencies and Tribal Nations to apply for read-only access to real-time data in the FCC's Network Outage Reporting System and Disaster Information Reporting System (September 2022)
- **Alerting Security:** Adopted a NPRM seeking comment on proposed rules to improve the security and operational readiness of the Emergency Alert System and Wireless Emergency Alerts (October 2022)
- **911 Outage Notification to PSAPs:** Adopted rules designed to ensure that 911 special facilities, including public safety answering points (PSAPs)/emergency communications centers (ECCs), receive timely and actionable information about 911 service outages. These rules standardize the type of information conveyed in notifications

and ensures that it is clear and actionable. It also requires service providers to maintain up-to-date contact information for the 911 call centers they serve (November 2022)

- **911 Location-Based Routing:** Released a draft NPRM on wireless 911 location-based routing to deploy technology that supports location-based routing on service providers' IP-based networks (November 2022)

### Cyber Resiliency in the 911 Environment

Chief Kopstein provided an overview of a recent cyberattack in a suburban New York county. In September, the county's integrated computer system suffered a ransomware attack that affected innumerable county operations. The attack disabled police department mobile data terminals, property tax collections, county payroll, and 911 computer-aided dispatch, and the hackers extracted and publicly posted decades of digitized, sensitive data. Chief Kopstein detailed the difficult recovery of the county, which had to borrow money to meet expenses and has yet to pinpoint when the system was infected, hindering the county's understanding of the attack's full impact. He noted that preventative measures, such as firewalls, protected several other communities despite their integration into the same system. He urged attendees to familiarize themselves with CISA cyber resiliency resources since preparation for cyberattacks affecting PSAPs can be complex.

Lisa Festa, CISA, echoed Chief Kopstein's sentiment and stated ransomware attacks, like the one experienced by this New York county, are a concern every community is facing. She elaborated on increased cyber risks to 911, noting that the advanced technology offered by Next Generation 911 (NG911) brings both additional benefits and risks. To provide the means to address the cybersecurity operation gaps that PSAPs face during NG911 transitions, CISA established the Cyber Resilient 911 (CR911) program. In 2022, CISA received Congressional appropriations funding with the instruction to enable a resilient NG911 ecosystem in partnership with the FCC, National Highway Traffic Safety Administration, and National Telecommunications and Information Administration. CISA is in the early stages of program development and does not have a preconceived solution in mind; as every PSAP is different, a one-size-fits-all solution is not viable. CISA is soliciting user involvement to ensure the CR911 program meets user needs and values SAFECOM members' input on program development. CISA will also use the upcoming SNS to identify PSAP cybersecurity gaps.

The following cybersecurity resources are available on the SAFECOM website:

- SAFECOM/NCSWIC Cyber Risks to NG911 White Paper
- SAFECOM/NCSWIC Two Things Every 911 Center Should Do to Improve Cybersecurity
- SAFECOM/NCSWIC Cyber Incident Response Case Studies for ECCs/PSAPs Suite
- CISA Cyber Risk to 911: Telephony Denial of Service
- CISA Public Safety Communications and Cyber Resiliency Toolkit
- SAFECOM "First 48": What to Expect When a Cyber Incident Occurs
- SAFECOM Guide to Getting Started with a Cyber Risk Assessment
- Emergency Communications Preparedness Center Considerations for Establishing Agreements for NG911
- CISA Stop Ransomware: Public Safety Emergency Communications Resources Webpage

**VISIT US AT:**

- cisa.gov/safecom/next-generation-911
- cisa.gov/safecom/technology
- cisa.gov/communications-resiliency
- cisa.gov/stopransomware/public-safety-emergency-communications-resources
- cisa.gov/safecom/ictapscip-resources

**Or email ng911wg@cisa.dhs.gov**

### Link Layer Authentication: Protecting Critical Communications Networks

Scott Wright, SAFECOM At-Large, State of Connecticut Department of Emergency Services and Public Protection, and Hermina (Nina) Koshinski, Chief of Radio Operations & Support for the Statewide Radio Network Division, Pennsylvania State Police, presented on a Project 25 (P25) system feature called Link Layer Authentication (LLA). LLA is a multi-factor authentication for LMR, which controls access to trunked radio systems by securely verifying a radio's authenticity prior to granting it system access. LLA is not encryption – it does not scramble messages being sent. It is a system validation process that uses a secret key function to validate legitimate subscribers before the radio is allowed to affiliate with a trunking system. A secondary advantage is the ability to disable a lost radio, if configured in the system, by preventing its

use by unknown entities. The cost of implementing LLA is relatively minimal and can be added to a mature system. For older radios, there may be a cost to add the LLA capability.

The system works by using a secret key to validate an authorized radio subscriber by assigning a unique authentication key associated with the subscriber radio's unit ID. The key is loaded into the subscriber radio and system with a P25 key fill device/interface. Authentication services are handled by an authentication application on the radio system. The authentication process initiates once the subscriber radio tries to register with the system. An authentication challenge is sent to the subscriber radio by the system. The subscriber radio returns a response assuming the radio has been loaded with the authentication key material. The radio system compares the subscriber radio's response and, if correct, authentication is successful and the subscriber radio is considered valid. If incorrect, authentication fails and the subscriber radio is denied access.


*Figure 1: LLA Functionality*

The presenters highlighted how the ease of using LLA is in stark contrast to the potential implications of lack of adoption by agencies. They provided use case examples from their own jurisdictions and promoted the use of LLA across all jurisdictions, agencies, and disciplines.

### Supporting Information and Communications Technology

Deputy Chief Lombard and Dan Wills, CISA, provided an update on changes to the National Incident Management System (NIMS) Incident Command System (ICS) to integrate information technology (IT) and cybersecurity positions into incident command and incident management organizational structures. The changes will be laid out in the *NIMS ICS Information and Communications Technology (ICT) Functional Guidance* document anticipated to be released in March 2023.

The ICT function within ICS can be managed by adding an IT Service Unit and/or a Cybersecurity Unit, along with the Communications Unit (COMU), into an ICT structure. This function could be included under the Logistics Section as a

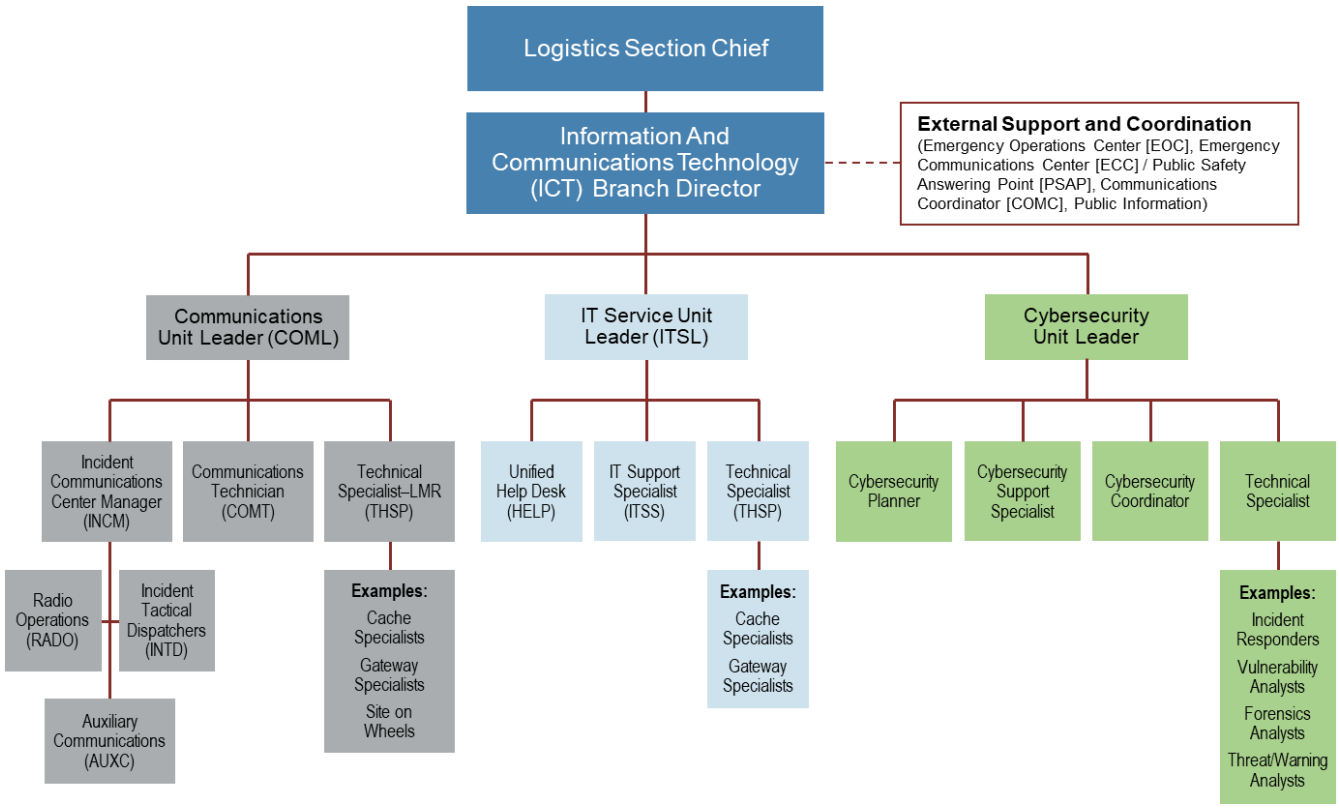


*Figure 2: ICT Branch Organizational Structure*

branch, under which the COMU is currently located. As depicted in *Figure 2*, an organizational structure was presented that depicted how a fully staffed ICT Branch under the Logistics Section could be established. Alternatively, according to NIMS doctrine, and depending on the needs of the incident and the command and general staff, management of the ICT function could be elevated to its own section.

The guidance document also includes the addition of the Cyber Unit and positions within that unit. Previously, a cyber planner position was included under the IT Service Unit Leader (ITSL). The Cyber Unit would be established to secure and protect incident communications but would not be designed to address other cyber impacts. This model is similar to the Medical Unit within the Logistics Section that supports incident responders, while emergency medical resources under the Operations Section provides services to the community.

The functional guidance document was developed by the Joint SAFECOM-NCSWIC Communications Section Task Force (CSTF), together with CISA and FEMA, and incorporated input provided by an Incident Communications Advisory Committee established under SAFECOM. Following the release of the functional guidance, the CSTF will work to refresh the Communications Unit Leader (COML) documentation, including its position description, position task book, and course curriculum. Additional positions will follow in the development process, including the ITSL position which has been in use through CISA guidance but not previously included as an ICS position.

### Critical Communications During Disasters: Response to Hurricane Ian

In late September 2022, Hurricane Ian, a strong Category 4 storm, struck Florida and South Carolina. The hurricane damaged countless properties, destroyed critical infrastructure, and required resource deployment to restore many of the government's identified Emergency Support Functions (ESF). Ultimately, every state in Region IV would experience the effects of Ian. Early in the incident, the decision was made to activate ESF #2 – *Communications* to prepare for the anticipated loss of critical communications infrastructure and services. Ms. Montanari moderated a panel discussion with local, state, and federal specialists who served on the ground in Florida to discuss how the restoration of emergency communications services and networks after Hurricane Ian was approached and executed.


*Figure 3: Path of Hurricane Ian, September 2022*

Roger Lord, Florida Statewide Interoperability Coordinator (SWIC), followed weather forecasts for two weeks prior to landfall and appointed a Communications Coordinator. Understanding their resources would be stretched after landfall, Ms. Montanari suggested seeking subject matter expertise from the State of North Carolina. Red Grasso, North Carolina Department of IT, a qualified COML, responded to help support Mr. Lord in accordance with an Emergency Management Assistance Compact request. Mr. Grasso noted that this deployment supporting ESF #2 was a very different experience from serving as a COML for an incident.

Several communications task forces were established around Florida, with each providing a COML, two Communications Technicians, a sworn law enforcement officer, and IT specialists along with two mutual aid radio caches equipped with subscriber units, a Radio Frequency Site on Wheels, and portable radio towers or repeaters. Sergeant Jason Matthews, Lake County Sheriff's Office, was assigned to lead a task force. These task forces interfaced with more than a half-dozen wired and wireless communications network operators to address service restoration for continuity of government, tactical communications, and dial tone as well as other provisions needed in the aftermath of the storm. Task forces were equipped to be largely self-sufficient (i.e., carrying their own food, water, and shelter) to minimize impact on already strained local resources. Deployed task forces quickly assessed what was and was not working when they arrived at their assigned locations. While this approach was effective, it exposed the need for more specialists to establish IT Service Units, and for

embedded amateur radio operators to provide auxiliary communications support. This resulted in more resources brought in from across the state and from out-of-state to meet these needs.

ESF #2 resources also helped restore 911 emergency telephone services, public safety communications networks, and commercial communications networks to help the public regain access to voice and data communications. Volunteers from the IT Disaster Resource Center in Texas deployed in support of dial tone restoration efforts. The commercial firm Rescue 42 responded and worked with other commercial vendors (e.g., Motorola Communications) to reconstitute destroyed local public safety networks. This was critical as Florida has a statewide public safety radio network but most localities are not participants. Telecommunicator Emergency Response Teams from Tennessee and Louisiana deployed to provide support and relief to Florida dispatchers, most of whom lost their homes from Ian's devastation. Both CISA and the FCC were mission-assigned to support ESF #2 from the state Emergency Operations Center and were supportive of all recovery and reconstitution efforts.

Task forces saw unanticipated requirements, including the need for aircraft and watercraft to reach work sites, large excavating equipment to move debris to gain access to critical infrastructure, and requests to restore cellular communications without specifying if the resources were needed to support government, public safety, or the general public. In hindsight, Mr. Lord suggested reaching out to tree services and fiber optic network operators ahead of the storm to support faster recovery operations and added that not every Internet Service Provider was represented (though they were invited; some chose not to send a delegate). Despite the challenges faced, the statewide network was restored within 72 hours – an amazing accomplishment.

### Engaging the Community in the SNS and National Emergency Communications Plan Update

Monica Watkins, CISA, highlighted the purpose of the SNS, which provides insight into national emergency communications needs and provides data that can be used by decision makers to inform programmatic, policy, and funding decisions. Considering the SNS data can be used to help justify funding, Ms. Watkins recommended that SAFECOM members encourage their associations and counterparts to participate. Deputy Chief Lombard echoed Ms. Watkins and reminded SAFECOM members that the SNS both sustains SAFECOM and makes a difference in the emergency communications landscape.

Mary Anne McKown, CISA Support, acknowledged CISA is currently awaiting Office of Management and Budget approval to commence SNS testing but anticipates that it will begin in early 2023. CISA will utilize a new survey platform to improve user experience. The SNS will be open for the entire public safety community's participation, as opposed to the 2018 survey which only targeted a random sample of local public safety organizations. Ms. McKown urged SAFECOM members to begin advertising the SNS within their associations to ensure the greatest amount of input from the public safety community once the survey goes live, and encouraged SAFECOM to reach out to CISA for assistance with SNS outreach, as needed.

Ms. McKown provided a preview of the National Emergency Communications Plan (NECP) update, congressionally mandated to occur every five years. The NECP establishes the nation's vision for emergency communications. Ms. McKown provided an overview of the phased process that CISA uses to update the plan. Deputy Chief Lombard and Ms. Watkins reiterated that the NECP justifies emergency communications funding, making it an essential tool for the public safety community. Ms. McKown requested attendees share emergency communications ecosystem challenges. Furthermore, she invited SAFECOM members to participate in and provide input through the upcoming NECP Working Group.

### Customizing Technical Assistance

Ken Carpenter, CISA Interoperable Communications Technical Assistance Program (ICTAP), informed members that Technical Assistance (TA) offerings are provided at no cost and include instruction and assistance with the planning, governance, operational, and technical aspects of developing and implementing interoperable communications initiatives. These offerings are designed to help emergency responders continue to communicate during disasters or large-scale planned events and support Statewide Communication Interoperability Plans (SCIPs) and the NECP.

Mr. Carpenter emphasized that each SCIP workshop and TA offering is tailored to the state's needs. Arkansas utilized the customization feature to build out a plan in preparation for the 2024 Solar Eclipse. The state is expecting 3.5 million visitors to experience the natural phenomenon and are working to ensure the infrastructure is capable to support that many users at one time.

CISA provides a Technical Assistance Service Offerings Guide (TA-SOG) and has expanded the resource as a direct result of stakeholder feedback. The TA-SOG provides a listing of CISA's TA services and products available to State, Local, Tribal, Territorial and Federal emergency communications partners to assist in areas such as Statewide Communications Interoperability Planning, Cybersecurity Awareness, Communications Plans and Standard Operating Procedure Development, and Training Courses for Incident Communications Personnel. Mr. Carpenter urged members to utilize the resources and to reach out and see what is possible to meet their needs.

### Trustmark Framework Update

Gabriel Martinez, CISA, and Matthew Moyer, Georgia Tech Research Institute, provided an update on the Identity, Credential, and Access Management (ICAM) Trustmark Framework. The Trustmark Framework endorsed by SAFECOM and NCSWIC in 2017 lacked the tools to implement it into a working Trust Federation to enable the public safety community to share information. To avoid a one-size fits all approach, the Framework scales up and adapts to the organization's needs.

The Framework's approach is to enable an ecosystem of assertion-based trust based on cybersecurity and ICAM principles. This level of trust will enable a peer-to-peer information sharing environment between public safety agencies. Open-source Trustmark Framework tools include:

- **Trust Policy Authoring Tool:** Used for publishing machine-readable artifacts that represent trust policy requirements
- **Trust Assessment Tool:** Used for performing Trustmark assessments and issuing Trustmarks
- **Trustmark Binding Registry:** Used for aggregating Trustmarks and binding them to system endpoints
- **Trustmark Relying Party Tool:** Used for making trust decisions and managing trust relationships based on Trustmarks

Mr. Martinez mentioned that with the tools operational and ready, governance discussions need to happen, and he plans to reach out to SAFECOM and NCSWIC leadership.

## SAFECOM SUB-GROUP MEETINGS

### Wednesday, December 14, 2022

In addition to the SAFECOM Meeting, members met to further collaborate on identified work products in the following subgroups:

- SAFECOM Governance Committee
- Communications Section Task Force
- User Needs Working Group
- SAFECOM Executive Board