SAFECOM NCSWIC

2019 **BIANNUAL SAFECOM MEETING**
Miami, Florida
November 5 & 6, 2019

Public Safety Strategic Collaboration Meeting

JOINT Meeting Executive Summary

Keynote: Cybersecurity and Infrastructure Security Agency's Deputy Director on Public Safety Communications

Speaker: Matthew Travis, Cybersecurity and Infrastructure Security Agency (CISA), Deputy Director (DDIR)

Objective: Convey CISA strategic focus areas and plans to work with public safety to address communications interoperability and cybersecurity issues now and into the future.

Key Points: DDIR Travis thanked SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) for being key partners with CISA. He emphasized CISA's commitment to supporting its stakeholders and the importance of its reciprocal relationship with the programs to develop best practices and guidance for the Federal, state, local, tribal, and territorial (FSLTT) public safety communications community. CISA recognizes the cascading, and influential, effects of SAFECOM's and NCSWIC's guidance down to the operational level and looks forward to continuing to strengthen its partnership with members as the organizations work together to make risk-informed decisions on emergency communications interoperability.

Photo: Matthew Travis, CISA Deputy Director

Improving Emergency Communications and Information Technology at an Incident

Photo: CISA and members of the ICAC pose following a meeting in March 2019

Speakers: Wes Rogers, CISA; John Miller, NCSWIC Chair (New Jersey); Paul Broyles, All-Hazards Incident Management Teams Association Board of Directors, Federal Emergency Management Agency (FEMA) Region X Representative; Tiffany Hudgins, FEMA, National Integration Center (NIC), National Incident Management System (NIMS) Implementation, Acting Branch Chief; Chief Chris Lombard, SAFECOM First Vice Chair, The InterAgency Board for Emergency Preparedness & Response, SAFECOM At-Large (Seattle Fire Department)

Objective: Learn about the Joint SAFECOM-NCSWIC Communications Section Task Force's (CSTF) and the Incident Communications Advisory Council's (ICAC) efforts to update the NIMS Incident Command System (ICS) to better manage communications and information technology at incidents and planned events. Learn how CISA is working to close gaps within NIMS ICS, including updating existing training courses, launching the Information Technology Service Leader (ITSL) course, creating new communications and information technology (IT) positions to support incident response, and incorporating IT positions from other organizations into the NIMS ICS structure.

Key Points: Presentations reminded the audience that within NIMS ICS, IT issues during incidents currently fall under the responsibility of the Communications Unit and provided an update on CSTF and the ICAC's collaborative efforts to gain support from the broader community and FEMA restructure communications elements of the system. Consensus-based recommendations coming out of both groups are twofold: 1) the Communications Unit and IT need to be organized under the same branch within ICS and the ITSL position should be adopted to lead the Information Technology Unit. Mr. Broyles provided additional background on why the ICS structure does not adequately support incident communications and data needs and emphasized the need to create a new unit for information technology. He reviewed key recommendations provided to FEMA NIC and acknowledged the challenge gaining consensus among relevant disciplines, but mentioned support is growing for their proposal. Ms. Hudgins stated their perspective on the proposal, including the establishment of a FEMA NIMS Coordination Group to facilitate conversations with stakeholders, like SAFECOM and NCSWIC, to create the Communications and IT Branch within the ICS structure. Chief Lombard noted the ICAC coordinated with FEMA NIC to include SAFECOM and NCSWIC as partners moving forward, which helps to fill public safety gaps in their current decision-making structure. Chief Lombard thanked those who sent letters of support for the initiative from their organizations and encouraged others to do the same.

Fireside Chat with FirstNet: User Interactions, Experiences, and Concerns

Speakers: Jeff Carl, AT&T, FirstNet Engineering & Operations, Director; Jacqueline Miller-Waring, First Responder Network Authority (FirstNet Authority), Regional Director; Paul Patrick, FirstNet Board Member, SAFECOM (National Association of State EMS Officials [NASEMSO] and SAFECOM At-Large, Utah Department of Health)

Objective: Participate in a moderated discussion with the FirstNet Authority and AT&T to ask pressing questions about current and future products and services.

Photo: Paul Patrick, FirstNet Board, SAFECOM Member; Jacqueline Miller-Waring, FirstNet; Jeff Carl, AT&T; Steve Devine, AT&T

Key Points: Participants engaged in an active discussion with the FirstNet Authority and AT&T on current and future products and services. Mr. Patrick introduced the panel and provided an update on the FirstNet experience, public safety engagement, and the FirstNet Authority budget for the upcoming fiscal year. Ms. Miller-Waring provided an overview of the FirstNet Roadmap, which gives a view of public safety's operational needs and technology trends for mobile broadband communications over the next five years. Mr. Carl provided an update on the current state of AT&T's support for the FirstNet network, and how as the network provider they are working to integrate commercial functionality into the dedicated public safety network core, while incorporating new capabilities at the request of stakeholders. Mr. Carl also highlighted new key features, like Mission Critical Push to Talk (MCPTT), and efforts to ensure the features operate under the standards established by the 3rd Generation Partnership Project (3GPP), as well as expanded coverage to the Pacific territories. Participants voiced concerns and asked questions to the panel, including interoperability with all cellular systems, incident priority versus uplift, and operations in close proximity to LMR systems. The FirstNet Authority provides other related resources through its website, such as Frequently Asked Questions and a fact sheet for download.

Improving your Cybersecurity Governance Posture: Cybersecurity Resources Available to the State, Local, Tribal, and Territorial Community

Speakers: Sean McCloskey, CISA Cybersecurity Advisor; Khristal Thomas, National Governors Association (NGA), Homeland Security & Public Safety Division

Objective: Learn about CISA's cybersecurity programs and NGA's ongoing efforts to improve cybersecurity governance and receive a comprehensive overview of resources available to the public safety FSLTT community to address organizational cyber risks.

Photo: Sean McCloskey, CISA, and Khristal Thomas, NGA, present FSLTT cybersecurity resources

JOINT Meeting Executive Summary

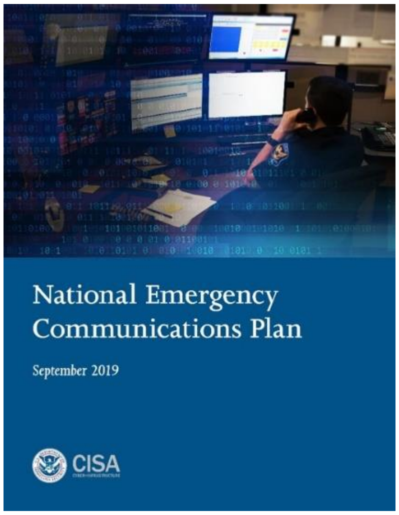
Key Points: SAFECOM and NCSWIC members learned about CISA's cybersecurity programs available to the public safety FSLTT community to increase organizational resilience against cyber risks NGA's ongoing efforts to improve cybersecurity governance. Mr. McCloskey discussed the Cybersecurity Advisory program under CISA and the resources available to the state/local public safety community, including access to CISA's Cyber Security Framework web resources, which stakeholders can use to enhance their cybersecurity posture; the Cyber Resilience Review, which includes guidance on how an organization can evaluate their operational resilience and cybersecurity practices of critical services; and, the Federal Virtual Training Environment (FedVTE), which provides free, online cybersecurity training to federal and FSLTT government employees, federal contractors, and veterans. Ms. Thomas then discussed how the public safety community can use the state model of a replicable framework for statewide interoperability communications and emphasized state and local partnerships that help raise awareness with local officials, conduct cyber trainings, and provide answers to questions from security providers.

Implementing the Updated National Emergency Communications Plan

Speakers: John Miller, Acting NCSWIC Chair (New Jersey); Michael Murphy, SAFECOM Second Vice Chair, SAFECOM At-Large (Baker, Louisiana, Police Department); Eric Runnels, CISA; Charlee Hess, CISA

Objective: Provide an overview of National Emergency Communications Plan (NECP) implementation planning, highlight SAFECOM's and NCSWIC's roles driving implementation, and discuss next steps.

Key Points: Mr. Runnels and Ms. Hess announced the release of the updated NECP and presented information on the newly-released revision to the NECP, including the collaborative stakeholder engagement process and key updates and additions since 2014. SAFECOM and NCSWIC are taking an active stance on implementing the priorities, including establishing a SAFECOM/NCSWIC Implementation Team to ensure progress toward the plan's recommendations. SAFECOM and NCSWIC leadership agree guidance coming out of the revised NECP will be reflected in the programs' Strategic Plans, which includes proposed product development and activities for calendar year 2020 and beyond. Mr. Miller and Mr. Murphy discussed the SAFECOM and NCSWIC input in the development of the NECP and announced the goals of the Implementation Team.



National Emergency Communications Plan

September 2019

CISA

Image: Cover of the 2019 National Emergency Communications Plan

Working Session: NECP Goal 6 - Interoperability Continuum Revision

Speakers: Jay Kopstein, SAFECOM (At-Large - New York State Division of Homeland Security & Emergency Services), SAFECOM-NCSWIC Interoperability Continuum Working Group Chair; Deante Tolliver, CISA

Objective: Receive an update on working group recommendations to revise the SAFECOM Interoperability Continuum to account for the evolution of data and voice communications. Attendees will participate in a working session to validate and provide further feedback on recommended continuum changes.

JOINT Meeting Executive Summary

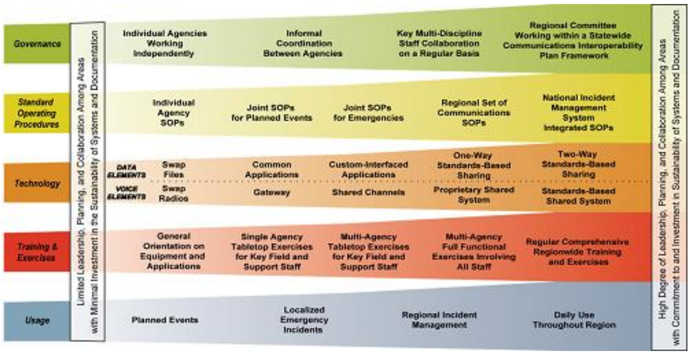

Governance
Standard Operating Procedures
Technology
Training & Exercises
Usage
Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation
Individual Agencies Working Independently
Informal Coordination Between Agencies
Key Multi-Discipline Staff Collaboration on a Regular Basis
Regional Committee Working within a Statewide Communications Interoperability Plan Framework
Individual Agency SOPs
Joint SOPs for Planned Events
Joint SOPs for Emergencies
Regional Set of Communications SOPs
National Incident Management System Integrated SOPs
DATA ELEMENTS
Swap Files
Common Applications
Custom-Interfaced Applications
One-Way Standards-Based Sharing
Two-Way Standards-Based Sharing
VOICE ELEMENTS
Swap Radios
Gateway
Shared Channels
Proprietary Shared System
Standards-Based Shared System
General Orientation on Equipment and Applications
Single Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Full Functional Exercises Involving All Staff
Regular Comprehensive Regionwide Training and Exercises
Planned Events
Localized Emergency Incidents
Regional Incident Management
Daily Use Throughout Region
High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation

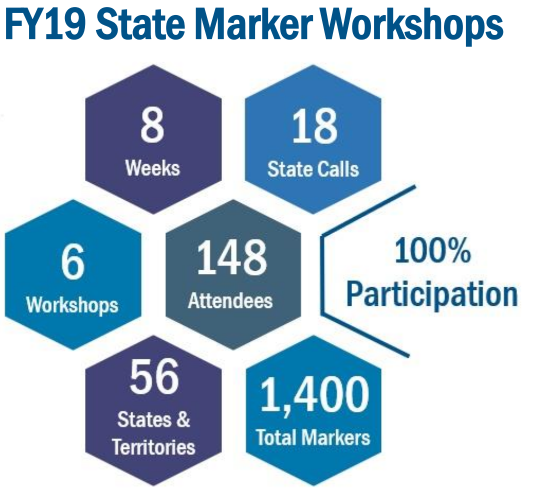
Image: SAFECOM Interoperability Continuum, 2014 version, *SAFECOM Website*

Key Points: The SAFECOM Interoperability Continuum is a legacy document designed to assist emergency response agencies and policy makers with planning for and implementing data and voice interoperability communications solutions. In 2019, SAFECOM established a working group under the Education and Outreach Committee to revisit the Continuum's content and assess its applicability in our ever-expanding and advancing emergency communications environment. The impetus for establishing the group also came on the precipice of the 2019 NECP revision release, within which recommendations are made to include cybersecurity in the Continuum as a critical element. Mr. Kopstein and Mr. Tolliver announced during the meeting that the Interoperability Continuum Working Group is seeking feedback and comments from SAFECOM and NCSWIC for updating the Interoperability Continuum. Most of the updates and modifications are found within the Continuum's Brochure text; specifically, the Governance and Standard Operating Procedures lanes of the Continuum. Mr. Tolliver and Mr. Kopstein led a working session to gather feedback on the updates. The group discussed the inclusion of additional lanes, including security. Mr. Tolliver and Mr. Kopstein will take the feedback to the working group for the next iteration. To provide additional recommendations on how to update the Interoperability Continuum to better reflect advancements or challenges in the current interoperability environment, email the SAFECOM Inbox at SAFECOMGovernance@HQ.DHS.GOV.

Using Data-Driven Decisions to Enhance Emergency Communications Interoperability

Speakers: Mark Grubb, CISA; J.L. Ellis, NCSWIC (Kansas); Don Bowers, CISA; Greg Hauser, NCSWIC (North Carolina)

Objective: Engage in a discussion on CISA's current performance management projects, including the NCSWIC State Interoperability Markers, Tribal Markers, Federal Markers, Incident Performance Measures, and a CISA-wide enterprise analytics project. Hear from stakeholders participating in these efforts and how to get further involved in data-driven initiatives in 2020.



Each of these efforts have helped contribute to the successful launch of the State Interoperability Markers by establishing a baseline of data for the nation.

Key Points: Mr. Grubb provided an update on the CISA performance management and data analytics programs, highlighting various interoperability markers initiatives. Every state and territory answered each of the 25 state markers questions, which measure emergency communications interoperability "health" at the state and territory level. Benefits of the interoperability markers review include the state's increased understanding of interoperability efforts, improved strategic planning, increased coordination across the state, and enhanced governance participation. Mr. Ellis noted that he measured Kansas' interoperability baseline differently than his statewide governing body because there was a systematic lack of communication among public safety stakeholders across the state. Mr. Bowers covered how the incident measures program, which stemmed from CSTF discussions, evaluates communications before, during, and after incidents. Mr. Hauser presented the draft incident measures in North Carolina and received positive feedback.

JOINT Meeting Executive Summary

Integration of Cellular Land Mobile Radio Gateways

Speakers: Jim Downes, CISA; Richard Schmahl, NCSWIC (Ohio), Ohio State Multi-Agency Radio Communication System, Program Director; Greg Hauser, NCSWIC (North Carolina), North Carolina Department of Public Safety; Roberto Mussenden, Federal Communications Commission (FCC)

Objective: Hear from stakeholders on how advances in broadband capabilities for public safety have led to integration challenges with statewide networks, namely capacity, security, and ensuring adherence to FCC requirements.

Key Points: Following instructions by Mr. Downes, Mr. Schmahl updated the group on broadband network implementation challenges in Ohio, specifically those regarding capacity and the difficulty in regulating and vetting new users joining the statewide system. Mr. Schmahl provided the FCC recommendations to address Ohio's issues. Mr. Hauser introduced North Carolina's statewide system and the challenges with rural and volunteer organizations using MCPTT applications in lieu of the more expensive option of outfitting all responders with radios, leading to the inability to track all users on the systems. Mr. Hauser suggested, when discussing access control solutions, states allow these communities to use MCPTT applications since investing in radios and infrastructure is not an option for many. Mr. Mussenden reminded users these are operational issues and controlling the system's capacity is a necessary step to address them. States facing unauthorized usage issues can contact the FCC ensure licensing organizations are meeting requirements mandating system user recognition, but Mr. Mussenden asked that states start implementing stronger control over the application users. First responders can be put at a security risk due to unauthorized users on the systems.

Migrating to 5G: Not Just an Upgrade

Speakers: Cindy Cast, Radio Systems Manager, Miami-Dade County Information Technology Department; Billy Bob Brown, Jr., CISA; Rob Dew, CISA

Objective: Hear from experts and users on the benefits and challenges of 5G for public safety mission critical systems.

Key Points: Mr. Dew informed members of 5G capabilities, benefits, and uses, which included an in-depth exploration of 5G technology and potential applications in a public safety environment. This exploration followed an overview of 5G research and field testing, commercial deployments, and standards development (e.g. 3GPP 5G Releases 15 and 16). Additionally, SAFECOM and NCSWIC were provided information on the timeline of projected 5G deployment and expected public safety impacts, including areas of concern. Mr. Dew urged emergency communications officials to be aware of 5G impacts on priority service, spectrum use, sharing, security, provisioning, and Internet of Things applications. Ms. Cast remarked that while 5G is not yet operational, 5G is conclusively arriving and emergency communications personnel should consider the impacts of commercial deployment of 5G on their critical infrastructure and city planning. Erecting 5G-supported sites could require months of planning and permitting. Ms. Cast also emphasized the importance of having investigative security capabilities, particularly as cyber and related threats endanger public safety communications systems. Mr. Brown reviewed 5G priority services standards.

Photo: Rob Dew, CISA; Cindy Cast, Radio Systems Manager, Miami-Dade County Information Technology Department; Billy Bob Brown, Jr., CISA

Identity, Credential, and Access Management Pilot: Enabling Secure and Mobile ICAM for Public Safety

Speakers: Todd Early, NCSWIC (Texas), Texas Department of Public Safety; Ted Lawson, CISA

Photo: Todd Early, NCSWIC (Texas), Texas Department of Public Safety; Ted Lawson, CISA

Objective: Hear recent CISA and Office of the Director of National Intelligence (ODNI) technical demonstrations designed to align public safety communities around common identity and access management practices that enable cost-effective, secure information-sharing in an operational environment.

Key Points: Mr. Lawson introduced recent work done by CISA, ODNI, SAFECOM, and NCSWIC on Identity, Credential, and Access Management (ICAM). Mr. Early emphasized the need to share information securely in a more streamlined fashion, which are the goals of the ICAM solutions proposed by this group. While the solutions exist, the public safety community needs more education on the topic to be able to make confident decisions with their information-sharing solutions. Mr. Lawson summarized ICAM as a way to validate that the end user has a need to know and should access that information in a trusted environment. The benefit of ICAM to the public safety community is to be able to share data with more organizations in a more efficient way. Mr. Early provided an update on the recent ICAM pilots conducted in Austin and Chattanooga, where organizations gave access to their systems using shared attributes in a trusted environment using the Trustmark Framework. During the pilots, two types of credentials were tested, FIDO and PIV-I. Mr. Early reviewed next steps for the group to provide additional outreach and educational materials to the public safety community on benefits and uses of ICAM.

Realizing the Value of Sharing Resources in Support of Public Safety Communications

Speakers: Dusty Rhoads, CISA; Mark Wrightstone, NCSWIC (Pennsylvania), Pennsylvania State Police Statewide Radio Network Division; Rob Zanger, Department of Justice (DOJ), Interoperability Coordinator

Objective: Listen to strategies being employed in support of a Shared Communications System and Infrastructure (SCSI) approach, whereby public safety organizations and their partners aim to enhance communications by sharing infrastructure, capabilities, and services in support of mission critical functions. Learn about ongoing SCSI initiatives—specifically, the Southwest Border SCSI project and the Pennsylvania Statewide Radio Network (PA-STARNet)—and how they promote reliable, resilient, operable, and interoperable communications for public safety users.

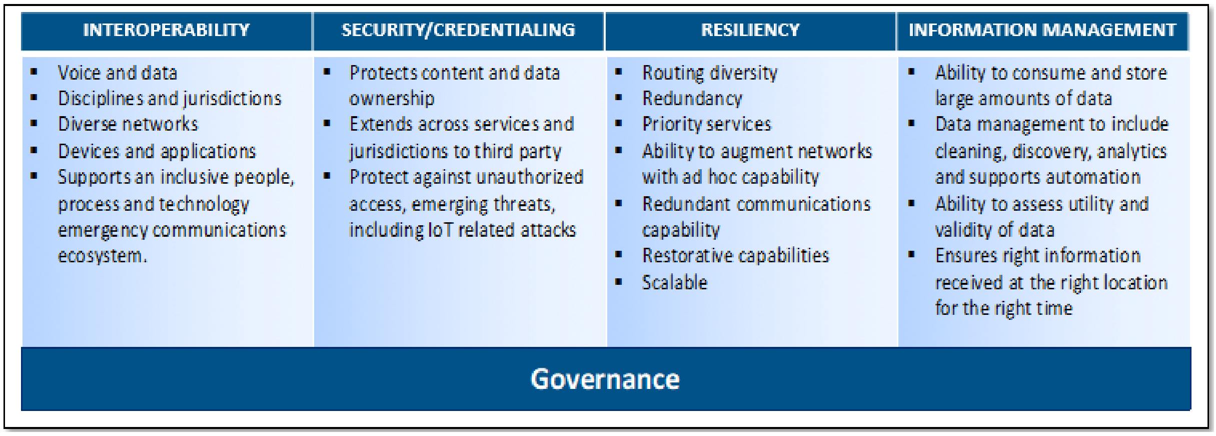
Key Points: Mr. Rhoads provided an overview of SCSI projects and the approach used at the southwest border. He highlighted the benefits of shared systems, such as increased operability and interoperability, optimized resource usage and management, and decreased duplication of investments. Mr. Wrightstone discussed PA-STARNet, a statewide system that allows users to subscribe to their system, including federal, state, and local partners. Mr. Zanger discussed how DOJ is working with states to subscribe to existing systems to save the department significant money and resources.

Information Sharing Framework Task Force Update

Speakers: John Contestabile, Washington Metrorail, Information Sharing Framework Task Force (ISFTF); Rob Dew, CISA; Chief Jonathan Lewin, (SAFECOM) Major Cities Chiefs Association

Objective: Receive a progress update from the ISFTF on establishing an Information Sharing Framework (ISF) as well as discuss technical and operational standards that enable secure information flow between public safety networks and systems.

Key Points: Chief Lewin introduced the topic and panel. Mr. Dew reviewed the background of the Task Force, explaining that the ISFTF had been formed after the April 2019 Joint SAFECOM-NCSWIC in-person meeting. The first Task Force call was held in July 2019, along with the first in-person meeting in August 2019. Given the complexity of sharing information when multiple organizations and agencies interact to complete their missions or respond to incidents, the ISFTF first established an Information Sharing Roadmap to identify information-sharing gaps for the Task Force to address. Mr. Dew and Mr. Contestabile shared the benefits of the ISF to public safety stakeholders. Mr. Contestabile also displayed how the Integration Layer, the link between data origination or storage and end user action, is the target of information sharing activity. The Task Force is currently reviewing a draft of the ISF, which is planned for broader SAFECOM-NCSWIC review.



INTEROPERABILITY	SECURITY/CREDENTIALING	RESILIENCY	INFORMATION MANAGEMENT
▪ Voice and data ▪ Disciplines and jurisdictions ▪ Diverse networks ▪ Devices and applications ▪ Supports an inclusive people, process and technology emergency communications ecosystem.	▪ Protects content and data ownership ▪ Extends across services and jurisdictions to third party ▪ Protect against unauthorized access, emerging threats, including IoT related attacks	▪ Routing diversity ▪ Redundancy ▪ Priority services ▪ Ability to augment networks with ad hoc capability ▪ Redundant communications capability ▪ Restorative capabilities ▪ Scalable	▪ Ability to consume and store large amounts of data ▪ Data management to include cleaning, discovery, analytics and supports automation ▪ Ability to assess utility and validity of data ▪ Ensures right information received at the right location for the right time
Governance			

Image: Key goals of the Information Sharing Framework Task Force

Supporting Inter- and Intra-State Mutual Aid: A Real-World Panel Highlighting Planning, Training, and Exercise Committee Resources

Speakers: Ben Bass, NCSWIC (Florida), Florida Division of Emergency Management; Michael Nix, NCSWIC (Georgia), Georgia Emergency Management and Homeland Security Agency; Jeb Hargrove, NCSWIC (Alabama), Alabama Emergency Management Agency; Greg Hauser, NCSWIC (North Carolina), North Carolina Department of Public Safety; Tommy Gonzalez, NCSWIC (Texas), Texas Department of Public Safety; Pam Montanari, CISA Region IV Coordinator – Moderator

Objective: Hear from a panel of experts on the value of preparing Emergency Management Assistance Compact (EMAC) Mission Readiness Package (MRP) Models prior to major hurricanes and learn about new materials assembled by the Planning, Training, and Exercise (PTE) Committee to support emergency preparedness and resource sharing, including the newly-launched COMM-X Portal.

JOINT Meeting Executive Summary

Photo: Ben Bass, NCSWIC (Florida); Michael Nix, NCSWIC (Georgia); Jeb Hargrove, NCSWIC (Alabama); Greg Hauser, NCSWIC (North Carolina); Tommy Gonzalez, NCSWIC (Texas); Pam Montanari, CISA Region IV Coordinator

Key Points: Ms. Montanari moderated a panel of Region IV Statewide Interoperability Coordinators (SWIC) on utilizing mutual aid during recent natural disasters. Each state discussed the use of EMAC requests during the 2019 hurricane season. Highlights included the need for states to be proactive identifying available resources to save time during emergencies when requesting and deploying resources. SWICs should build strong relationships with neighboring states to understand their capabilities and resources and ensure communications with the state EMAC coordinator to understand the processes and leverage their expertise. Additional suggestions included engaging with media during early stages of emergency response to leverage their coverage and including vendors in the Emergency Support Function (ESF)-2 process. Mr. Gonzalez closed out the discussion by reviewing products developed by the NCSWIC PTE Committee to support states during mutual aid situations, including the six EMAC MRP templates to account for equipment, resources, and costs, and a best practices document to help states prepare for EMAC requests. These documents can be found on the NCSWIC website and the COMM-X Portal, an online database of training and exercise resources. To request access to the portal, email comm.xportal@hq.dhs.gov.

If you haven't done so already, please provide CISA feedback on your meeting experience!