SAFECOM

NCSWIC

Spring 2021 Virtual Engagements

May 4 - 6 | May 11 - 13

MAY 4-6, 2021 SESSIONS

- Emergency Communications Lessons Learned from the Nashville Christmas Bombing
- Location Accuracy in the Field using Geographic Information Systems
- Location Accuracy Part II: Vertical Z-Axis Requirements
- What's New in Emergency Communications Grant Funding?
- State Markers Update
- CISA Update: 5G and Priority Telecommunications Services

MAY 11-13, 2021 SESSIONS

- Responding to Cyber Incidents: What to Expect?
- Cybersecurity Planning for Emergency Communications: What Does the Future Hold?
- Support for Vaccine Distribution Centers
- January 2021 Presidential Inauguration Follow Up
- Expecting the Unexpected: Short-Term Planning and Emergency Communications Support for Civil Disturbances
- Auxiliary Emergency Communications Update
- Lunch with Leaders: CISA Executive Assistant Director for Cybersecurity
- Expanding Broadband Access and Connection to Rural and Tribal Communities
- Texas Winter Storm 'Uri' Communications Impacts
- Collaborating on Mutual Aid for Long-Term Evolution (LTE) Mission Critical Push-to-Talk

Visit the website to find more information on SAFECOM's and NCSWIC's products and events:

cisa.gov/safecom

On May 4th, 2021, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) kicked off their bi-annual meeting. Conducted virtually for the second time, multiple informative and productive sessions took place over the course of a two-week period. The Cybersecurity and Infrastructure Security Agency's (CISA) Deputy Director (DDIR), Nitin Natarajan, helped kick off the event by serving as the keynote speaker and providing opening remarks and CISA updates.

Members of both organizations selected topics for this year's engagement series, focusing on the groups' most pressing priorities. Session topics included critical communications infrastructure impacts from both natural and man-made disasters; advancements in location accuracy; solutions for managing an increasing number of cyber threats; best practices for mass vaccine distribution and other real-world events; and efforts to expand broadband access.

Face-to-face interaction and networking are cornerstones of SAFECOM and NCSWIC's regular in-person meetings. Given these unprecedented times, these virtual engagements also offered opportunities to meet new members and share stories.

KEYNOTE: CISA DEPUTY DIRECTOR NITIN NATARAJAN

CISA DDIR Nitin Natarajan provided the keynote address to officially kick off the Spring 2021 SAFECOM and NCSWIC virtual engagement. DDIR Natarajan acknowledged SAFECOM and NCSWIC as key CISA stakeholders in driving advancements to emergency communications capabilities. The DDIR commented,

"The outstanding work you have done has readied your communities to respond more effectively during this unprecedented time, while current and future initiatives continue to assure progress in the field. These successes are a direct result of your programs' strong foundation and footprint in the community."

During his remarks, the DDIR shared key CISA updates, discussed stakeholder-driven priority topics, and provided a forum to hear about critical communications infrastructure impacts.

ACCESS VIRTUAL ENGAGEMENT SESSION RECORDINGS!

Please contact the SAFECOM Inbox or NCSWIC Inbox with questions or feedback.

EMERGENCY COMMUNICATIONS LESSONS LEARNED FROM THE NASHVILLE CHRISTMAS BOMBING

May 4, 2021

Within the first few hours of a bomb explosion in Nashville, Tennessee, the morning of December 25, 2020, the incident did not appear to have any major impacts on emergency communications, even with a commercial carrier service facility impacted, according to Stephen Martini, Metro Nashville Department of Emergency Communications, and Christine Massengale, Tennessee Dispatch Coordinator. However, as generators failed to respond due to technical issues and backup battery power was depleted, the incident quickly turned into a multi-jurisdictional, multi-state problem that disrupted Public Safety Answering Points (PSAPs) and commercial cellular service for days. A quick response by commercial and mutual-aid partners to provide backup power within hours and deploy more than two dozen Cell on Wheels (COW) and Satellite Cells on Light Trucks (SatCOLT) to the area within the first couple of days proved effective. Mike Sunseri, Kentucky Office of Homeland Security, and Brandon Marshall, Kentucky State Police, described how Kentucky was able to quickly capture data on PSAPs and 911 dispatch centers that were experiencing service disruptions and incomplete 911 calls—an effort that proved crucial to Kentucky's response and assessment of the impacts. Among the states and agencies impacted, several lessons learned—such as improving coordination with commercial partners, strengthening processes for reporting service outages, and sharing continuity of operations plans (COOP) among mutual-aid partners—came to the forefront as the widespread impacts of the bombing on the public safety community became apparent in its aftermath.

Figure 1: ***Public Safety Communications Dependencies on Non-Agency Infrastructure and Services*** **provides several examples of infrastructure and service dependencies that public safety agencies might have on non-agency entities.**

The First Responder Network Authority (FirstNet Authority) recognized the challenges the public safety community was experiencing and formed a crisis team in response, meeting with over 50 agencies impacted by the incident. Assessments performed by public safety agencies, federal government, and commercial partners revealed the primary challenge was not a communications hardware issue but rather a power issue, as the commercial service facility itself and communications infrastructure were not critically damaged. Dependencies on critical infrastructure outside the control of public safety communications, such as access to sustainable power, became a focus of the agencies as a result of the incident. In 2020, SAFECOM and NCSWIC published a document—*Public Safety Communications Dependencies on Non-Agency Infrastructure and Services*—to help agencies understand what steps can be taken to prevent or mitigate operational disruptions due to failures or downtime of infrastructure dependencies.

LOCATION ACCURACY IN THE FIELD USING GEOGRAPHIC INFORMATION SYSTEMS

May 5, 2021

Mr. Joshua Black, CISA and federal lead for the SAFECOM Next Generation 911 (NG911) Working Group, facilitated a session focused the geographic information system (GIS) lifecycle and best practices and resources for implementing GIS capabilities. Speakers discussed the benefits of GIS capabilities to the public safety community and the importance of GIS for the implementation of NG911.

Mr. Budge Currier, California Statewide Interoperability Coordinator (SWIC), shared how California implemented a robust GIS system and how he engaged with state, local, and tribal partners to identify GIS requirements. Ms. Margaret Montgomery, GIS Manager, City of Manassas, Virginia, discussed how the City of Manassas implemented GIS capabilities for NG911 and collaborated with the state and neighboring jurisdictions to establish GIS boundaries. Ms. Laurie Flaherty, Coordinator, National 911 Program, U.S. Department of Transportation, provided an overview of GIS implementation for NG911 across the Nation.

Panelists answered questions from participants about standard addressing schemes, cybersecurity best practices for GIS and NG911, and how GIS supplemental data works with RapidSOS. Panelists noted they were not endorsing a particular product or vendor solution.

Ms. Flaherty shared GIS resources, including the SAFECOM and NCSWIC GIS Lifecycle Best Practices Guide for NG911, California Statewide NG911 GIS Use Case, City of Manassas, Virginia GIS Use Case, the NG911 Self-Assessment Tool, and the National 911 Program's NG911 Roadmap.

LOCATION ACCURACY PART II: VERTICAL Z-AXIS REQUIREMENTS

May 5, 2021

Mr. Black also facilitated a discussion on vertical location, or "z-axis," data and how the public safety community can use this altitude-based metric to improve emergency response and save lives.

Ms. Erika Olsen, Senior Counsel, Public Safety and Homeland Security Bureau, Federal Communications Commission (FCC), discussed the evolution of z-axis and FCC requirements for vertical location data for wireless 911 calls. The FCC established requirements for carriers to provide vertical location data within 3 meters for 80% of wireless 911 calls, resulting in more consistent data.

Mr. Tyrell Morris, SAFECOM At-Large member and Executive Director, Orleans Parish Communication District, discussed the impact of z-axis data on telecommunicators and how public safety agencies can prepare for receiving this data. Mr. Morris shared how New Orleans is using existing GIS data, maps, elevation data, and satellite imagery to construct a three-dimensional model of the city to help 911 centers pinpoint locations in elevated buildings. He also discussed the importance of training telecommunicators for receiving vertical location data and sharing it with first responders in the field.

Mr. Steve McMurrer, 911 Systems Administrator, Department of Public Safety Communications, Fairfax County, Virginia, discussed efforts by organizations, such as the National Emergency Number Association (NENA), to develop requirements and standards to improve how 911 carriers provide vertical location data. He spoke about the importance of establishing requirements and consistent language to ensure data is actionable and useable by 911 centers. Members discussed challenges with collecting, sharing, and maintaining vertical location data, as buildings often have differing heights and floor numbers. Mr. Morris stated that as technology evolves, New Orleans plans to use school floor plans to articulate height. Members discussed opportunities for SAFECOM and NCSWIC to provide feedback to the FCC to help develop policies to ensure carriers are providing the information public safety

VIRTUAL CAFÉ: LET'S PLAY JEOPARDY!
May 5, 2021

What's New in Emergency Communications Grant Funding?

SAFECOM and NCSWIC members reviewed information on new emergency communications funding opportunities and resources through an interactive gaming session, including new National Telecommunications and Information Administration (NTIA) grant opportunities, key funding updates, and available resources.

Three new NTIA grant programs are under development to support broadband initiatives and investments. The $300 million **Broadband Infrastructure Grant Program**, the $1 billion **Tribal Broadband Connectivity Grant**, and the $285 million **Connecting Minority Communities Pilot Program** are expected to be released by NTIA this summer. Members are encouraged to attend NTIA's Broadband Grant Programs Webinar Series to learn more. Key funding updates included information on the T-Band auction reversal, the FCC's recent 911 Surcharge Notice of Proposed Rulemaking, and the new mandatory 7.5 percent cybersecurity spend for the Homeland Security Grant Program. CISA also reminded members of available funding resources including the *SAFECOM Guidance on Emergency Communications Grants*, the *List of Federal Financial Assistance Programs Funding Emergency Communications*, and the upcoming *Funding Mechanisms Guide for Public Safety Communications*.

agencies need. Participants on the location accuracy panels did not endorse, recommend, or make representations with respect to a product or vendor solution.

VIRTUAL LUNCH AND LEARN: STATE MARKERS UPDATE

May 6, 2021

Mark Grubb, CISA, provided an overview of the State and Territory Interoperability Markers Program, including background on the development of the markers and next steps for states. In 2019, CISA worked closely with states and territories to develop a set of 25 markers that gauged "interoperability maturity" on governance, standard operating procedures (SOP), technology, training and exercises, and usage to show how interoperability is progressing nationwide.

Each state and territory conducted a self-assessment, assessing itself as either initial (has not made any progress in that marker), defined (meets some of the marker criteria), or optimized (meets all of the marker criteria). On at least an annual basis, CISA requests that states provide updates to their assessment, noting many states utilize the statewide interoperability governing bodies to help.

CISA then incorporates the data into an enterprise analytics dashboard to track the progression of interoperability over time and to show any gaps *(Figure 2)*; although CISA is tracking each marker, there are no time constraints in place that states need to meet.

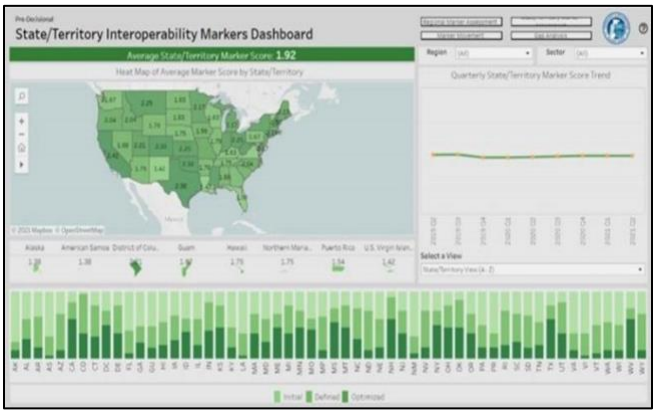

Figure 2: CISA enterprise analytics dashboard to track progression of interoperability and show gaps.

CISA categorizes any marker with more than 35% of states self-assessing in the "initial" category as a "high percentage gap," because it presents more risk for interoperability. The gaps are then used by the Interoperable Communications Technical Assistance Program to develop individualized trainings and to update Statewide Communication Interoperability Plans. There are currently ten "high percentage gap" markers. As a next step, CISA is creating a Risk Register to help identify risks to emergency communications using the marker data. More information on the new program will be available in late 2021.

CISA UPDATE: 5G AND PRIORITY TELECOMMUNICATIONS SERVICES

May 6, 2021

The 5G service architecture is complex, and a host of elements must be taken into account when looking to provide end-to-end priority services, according to CISA's Navin Jaffer, Next Generation Networks (NGN) Priority Services, and Rob Dew. The transition, with a schedule unique to each carrier, involves priority services expanding beyond just voice services—as is the case with 4G—and into data, video, and information service offerings. 5G priority services differ from 4G priority services in several ways: spectrum resources and spectrum allocation will be much greater, long-term evolution (LTE) can be better leveraged, battery life will improve, and more features will be available through cloud computing.

Changes to priority services are being made in three phases: Phase 1, ensuring priority in voice in wireless networks; Phase 2, providing data, video, and information priority, which may take several years; and Phase 3 is 5G voice. Given the current trajectory, 5G services are expected to become available first to population-dense areas such as major metropolitan areas, though many concerns about line-of-sight and signal obstruction remain. Within CISA, the NGN Priority Services team is working with providers to ensure that seamless Wireless Priority Services (WPS) performance, cybersecurity controls, and interoperability across service providers are included in the 5G transition, and that the process remains stakeholder driven as commercial providers follow the Phase 1, Phase 2, and Phase 3 continuum.

SAFECOM BUSINESS SESSION

May 6, 2021

Chief Gerald Reardon, SAFECOM Chair, welcomed new SAFECOM members, including two new associations: All-Hazards Incident Management Teams Association and DRONERESPONDERS Public Safety Alliance; four new at-large members; and two new association representatives for the National Association of State EMS Officials (NASEMSO) and International Association of Fire Chiefs. Chief Reardon presented the 2021 Marilyn J. Praisner SAFECOM Leadership Award to Mr. Kevin McGinnis, who, since 2003, has contributed significantly to SAFECOM's effectiveness in his role as NASEMSO representative. Chief Jon Olson provided a SAFECOM Member Spotlight presentation on the National EMS Management Association (NEMSMA), a professional association of EMS leaders from various disciplines (e.g., law enforcement, fire, military) focused on enhancing EMS systems. NEMSMA represents 34 states, plus Ontario, Canada, and Abu Dhabi, and is comprised of 465 individual members and 279 agency members. The organization's four big initiatives include a field training and evaluation program, paramedic officer credentialing, EMS/hospital data sharing, and EMS publications.

Figure 3: Mr. Kevin McGinnis, 2021 Awardee, Marylin J. Praisner SAFECOM Leadership Award.

Figure 4: SAFECOM Member Spotlight: NEMSMA.

SAFECOM subgroups and representatives of the federal community provided updates on their recent initiatives. Mr. Russell Becker, Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Office for Interoperability and Compatibility (OIC), shared information on a FirstNet push-to-talk (PTT) field trial, which aims to provide DHS-component end-users with the opportunity to test handsets in a standards-compliant, mission critical PTT application and test usability and performance. He also shared a video link from S&T on potential Automated Speech Recognition technology solutions. Mr. Rob Zanger, Department of Justice (DOJ), presented on a series of DOJ wireless communications studies going back to 1999, all of which identified a role for commercial wireless offerings in meeting DOJ's requirements.

NCSWIC BUSINESS SESSION

May 6, 2021

Figure 5: NCSWIC Vice Chair and Michigan SWIC, Brad Stoddard

John Miller, NCSWIC Chair and New Jersey SWIC, welcomed new members of the SWIC community, including four new SWICs and three new Deputy SWICs, and thanked his fellow SWICs and CISA for their continued perseverance and support during the last year. Brad Stoddard, NCSWIC Vice Chair and Michigan SWIC, presented on Michigan's State-of-the-State and provided a history of emergency communications in his state, emphasizing the rapid changing pace of emergency communications. Mr. Stoddard shared how states can leverage technology to fill gaps in funding or manpower. Greg Hauser, North Carolina SWIC, and Travis Johnson, Louisiana SWIC, presented on their respective states' efforts to develop dashboards to collect and analyze data during events. Mr. Hauser and Mr. Johnson shared features included in their dashboards *(Figure 6)*, such as locations of communications equipment and weather events. CISA indicated they would be willing to facilitate future information sharing conversations between members about next steps to develop their own dashboard.

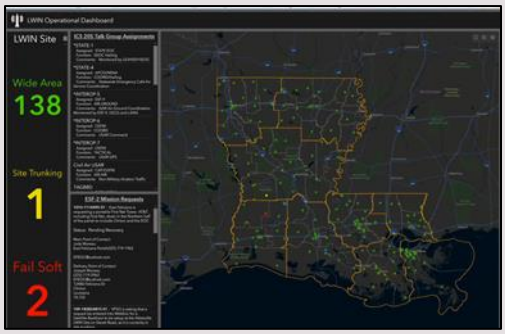

Figure 6: Louisiana Wireless Information Network Operational Dashboard

Additionally, Marty McLain, CISA Eastern Sector Branch Chief, spoke about CISA's technical assistance (TA) offerings in the time of COVID. CISA is still offering TAs, however most are virtual. Should you require an in-person TA, you can contact the Emergency Communications Division (ECD) with the request. Mr. McLain did caution it is a lengthy process and to contact ECD as soon as you know you may require assistance.

RESPONDING TO CYBER INCIDENTS: WHAT TO EXPECT?

May 11, 2021

Mr. Ted Lawson, CISA federal lead for the SAFECOM Cybersecurity Working Group, introduced Working Group co-chairs, Mr. Mark Hogan, SAFECOM At-Large member, City of Tulsa, Oklahoma, Department of Asset Management, and Captain George Perera, SAFECOM At-Large member, Miami-Dade Police Department. The session focused on what to expect after a cyber incident has occurred, and—using the recent ransomware attack against the City of Tulsa as an example—the techniques and mitigation efforts related to incident response and recovery, as well as resources and services that can assist public safety organizations.

Mr. Hogan presented a timeline of the cyber incident response process and walked through the necessary steps his department took to detect, respond to, and recover from the incident. Mr. Hogan was notified by the Federal Bureau of Investigation (FBI) of the potential existence of ransomware on his network. He worked closely with his team, via the pre-established cyber incident response team process, to scan the network, locate the malware, shutdown the network and systems, maintain business and operational continuity, and continue to recover from the ongoing incident. The team brought on vendor support to help with a variety of efforts (e.g., network analysis and forensics). In addition, they notified the state's chief information security officer, CISA, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the United States Computer Emergency Readiness Team (US-CERT).

RESPONDING TO CYBER INCIDENTS

Mitigation and Response Steps

- Have a response plan in place that includes pre-identified stakeholders, support, and resources
- Ensure redundancy, especially of resources, as the availability of aid and assistance could vary depending on a variety of factors (e.g., incidents of higher priority and/or urgency)
- Engage CISA for a variety of cybersecurity service offerings
- Leverage third-party vendors and contract support to assist cyber incident response in a timely manner
- Consider network decentralization to mitigate malware from affecting entire systems in the event of a breach

Mr. Hogan emphasized the importance of securing backups and ensuring backup redundancy. In the Oklahoma incident, it was difficult to restore and rebuild systems from backups when the team had to shut down their backup system as a part of the mitigation process. Mr. Hogan was unable to receive federal assistance as his incident coincided with the Colonial Pipeline ransomware attack. He suggested streamlining the reporting process, as he had to fill out separate reporting forms for the MS-ISAC and US-CERT. Other participants echoed that organizations should be prepared to defend their networks and systems by themselves in the initial period and that they should also be trained in using backup plans if networks are compromised. Mr. Hogan clarified that Cisco's Advanced Malware Protection (AMP) tool was used to scan the network, his department did not pay a ransom, and an email attachment was possibly exploited in the attack.

The SAFECOM Cybersecurity Working Group is developing resources to guide public safety organizations in cyber incident response. Additional pending publications developed to help the community include a cybersecurity insurance fact sheet, whitepaper on cyber risks to land mobile radio (LMR), and a guidance document on cyber risk assessment. Mr. Lawson reminded participants to check out existing SAFECOM-NCSWIC and CISA resources, such as CISA's ransomware resources, for additional guidance and support.

CYBERSECURITY PLANNING FOR EMERGENCY COMMUNICATIONS: WHAT DOES THE FUTURE HOLD?

May 11, 2021

The Communications Section Task Force (CSTF) is working to define current and future cyber capabilities needed during all-hazards incident response. Cybersecurity threats have been realized in public safety communications, law enforcement, and fire and emergency services in the form of natural, intentional, and accidental incidents. There are indications these sorts of problems will

increase as our adversaries develop more methods to disrupt, damage, or destroy communications resources at planned events, emergencies, and incidents. SAFECOM members and SWICs participated in a working session to share their recommendations on how to best prepare for and protect all-hazards incident communications from cybersecurity disruptions. Many members voiced the need for more cybersecurity education and training, adoption and implementation of the Information Technology Service Unit Leader (ITSL) position, and more extensive cybersecurity planning. In the future, members anticipate experiencing more cyber radio, 911, and jamming disruptions, as well as more coordinated multi-threat attacks (e.g., intentional ransomware attack simultaneous with an all-hazards incident). With the information gathered from the discussions, the CSTF will work with CISA to explore and develop solutions to cybersecurity threats that emerge during response to or recovery from all-hazards incidents.

VIRTUAL LUNCH AND LEARN *May 12, 2021*

Support for Vaccine Distribution Centers

John Miller, New Jersey SWIC, and Shelly McMahon, California Deputy SWIC, led a discussion on lessons learned during the deployment of communications at mass vaccine distribution centers. Building on lessons learned setting up Alternate Care Sites last year, they first established communications capabilities at each site, determined which carriers had the best service, and identified the type of devices needed. New Jersey and California focused the majority of vaccine distribution efforts towards large state-run mass vaccination sites and smaller community-based sites in under-served areas, including the use of mobile vaccination vehicles.

One of the biggest take-aways from the last year was the need for redundancy in equipment and personnel. When an incident lasts for months, personnel can quickly get burnt out and it is important to have enough trained personnel to mitigate the loss of redundancy. Some other lessons learned in New Jersey and California included:

- Ensure trained staff are available to help with the establishment of large sites
- Utilize CISA TA offerings to train Communications Unit Leaders and ITSL
- Mitigate communications issues by providing various communications methods up front, including devices with dual-SIM capabilities, cache radios, and the ability to hardwire laptops in case of Wi-Fi overload
- Stagger the deployment of each site to understand each site's communications needs
- Build and maintain relationships at federal and SLTT levels

JANUARY 2021 PRESIDENTIAL INAUGURATION FOLLOW UP

May 12, 2021

Tom Gagnon, CISA Eastern Sector Coordinator, facilitated a discussion on planning for the January 2021 Presidential Inauguration and how the District of Columbia (DC) worked collaboratively with neighboring jurisdictions and federal partners to support the National Special Security Event. Charlie Guddemi, DC SWIC, discussed their five-month planning process and how they addressed challenges, such as ramping up Primary, Alternate, Contingency, and Emergency (PACE) planning after the Nashville Christmas Day bombing. Recognizing that the current National Incident Management System (NIMS) Incident Command System (ICS) was insufficient to support the large-scale event, he discussed how DC established a three-branch communications section to ensure communications operability and interoperability.

During the discussion, panelists shared lessons learned from the event. Master Sergeant (MSgt) Samuel Hoover, Washington, DC, Air National Guard, spoke about how the Air National Guard adjusted their communications plan to accommodate the expanding deployment of more than 27,000 troops. Mike Baltrotsky, Assistant Fire Chief, Montgomery County, Maryland, Fire & Rescue, described the National Capitol Region (NCR) Communications Interoperability Group's contributions and joined Charles Bryson, Maryland FiRST Technical Advisor, Maryland Department of Information Technology and Chair, FCC Regional Planning Committee 20, to discuss how the deployable trunking system for the NCR can provide additional capacity for their radio system. Mr. Bryson highlighted how they developed a standardized interoperability template for Region 20 to ensure interoperability and redundancy across mutual aid partners.

EXPECTING THE UNEXPECTED: SHORT-TERM PLANNING AND EMERGENCY COMMUNICATIONS SUPPORT FOR CIVIL DISTURBANCES

May 12, 2021

Steve Noel, CISA Western Sector Branch Chief, led an interactive discussion between MSgt Samuel Hoover, Washington, DC, Air National Guard, and Kenneth Link, Jr., DOJ Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), on how to plan for unplanned incidents with little lead time and the differences in response and recovery compared to planned events. The number one factor that often determines the success or failure of response to a "no-notice" incident is the strength of federal, state, local, tribal, and territorial (SLTT) partnerships. Partnerships are critical to interoperability. When possible, it is beneficial to complete training and exercises with partners that may support response to a large incident. This helps build trust between public safety personnel and allows responders to become familiar with the equipment and skills other public safety organizations can offer.

Panelists discussed the modifications needed when moving from long-term planning for events, to short-term planning for no-notice, large-scale public incidents. MSgt Hoover emphasized the importance of utilizing pre-existing plans, which allow incident leadership to scale up or scale down a plan based on the severity and size of the no-notice event. Additionally, public safety entities should always have a backup plan. Panelists also mentioned the use of web conferencing tools, such as Microsoft Teams, and the benefits they provide to quickly connect and share information in real time. Participants also spoke to the importance of encryption. Encryption is like interoperability in that it is managed locally and employs national standards and best practices. DOJ policy mandates the use of encryption 100 percent of the time, but this is often difficult to achieve as most local departments do not have equipment that can support encryption. This underscores the importance of establishing relationships with partners to understand available equipment and develop a plan to secure incident communications. At the end of the session participants had a better understanding of how to plan and train for unplanned events that require encryption, operational security, physical security of deployable assets, and flexibility.

AUXILIARY EMERGENCY COMMUNICATIONS UPDATE

May 12, 2021

Karla Jurrens, Auxiliary Communications (AUXCOMM) Working Group Chair and Texas Deputy SWIC, provided updates on the number of AUXCOMM classes which have been conducted, as well as planned and completed Working Group efforts.

Originally developed in 2009, the AUXCOMM course provides an overview of the AUXCOMM position, including the responsibilities, roles, and functions within the Communications Unit (COMU), as well as roles and functions of the Auxiliary Communicator (AUXC) within NIMS ICS. Since then, the AUXCOMM program has taught the course 154 times by both CISA and state-sponsored instructors, with over 3,000 students trained to date. There are currently 29 qualified state-sponsored AUXCOMM instructors nationwide, with an additional 12 state-sponsored instructors close to certification.

In 2019, the CSTF saw the need to update the AUXCOMM course and established the AUXCOMM Working Group. The Working Group is currently updating the Auxiliary Field Operations Guide (AUXFOG) and developing supplementary materials to continue the AUXCOMM mission. To date, the AUXCOMM Working Group has completed the following:

- *Auxiliary Communicator Position Task Book* – Documents performance criteria a trainee must meet to be certified for the AUXCOMM position
- *AUXCOMM 509 Form* – Details the official position description
- *Contributed to the Updated Field Operations Guide App* – Publication expected to coincide with the release of the National Interoperability Field Operations Guide (NIFOG)

Further, the Working Group intends to develop:

- *AUXCOMM Communications Exercise (COMMEX)* – Certifies an individual taking AUXCOMM at the state level

- *AUXCOMM Digital Mobile Radio (DMR) Network* – A voice network using amateur radio service with talk groups that are state and/or DHS region specific
- *AUXCOMM Fusion Center* – A virtual tool, tentatively named, to enable COMUs to share information about deployed systems and team composition during an actual event affecting a state or region

LUNCH WITH LEADERS: CISA EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY

May 13, 2021

Eric Goldstein, CISA Executive Assistant Director (EAD) for Cybersecurity, participated in a fireside chat with NCSWIC Chair, John Miller, New Jersey SWIC. With a background as a firefighter for 15 years, EAD Goldstein comes to the cybersecurity space through the lens of emergency management. He provided remarks on recent CISA cybersecurity campaigns, including "Reduce the Risk of Ransomware" *(Figure 7);* the importance of ensuring the security of our Nation's critical emergency communication systems; and CISA's cybersecurity services and programs that can be utilized by emergency communications responders.

EAD Goldstein outlined three core goals for CISA:

1. Be the first touchpoint for the public safety community, whether it be for risk assessments or cyber advice. He encouraged stakeholders to utilize CISA's regional cybersecurity advisors and available technical assistance. Additionally, he noted SAFECOM and NCSWIC are considered core constituents
2. Focus on functional resilience, while also being focused on security. Even the best organizations may have vulnerabilities. Adversaries may spend years and millions of dollars to compromise infrastructure. Stakeholders need to plan for the worst-case scenarios
3. Ensure an open line of communication between the public safety community and CISA's Cybersecurity Division (CSD). CSD is committed to building useful tools for stakeholders and to working across CISA Divisions, especially ECD, to make sure services are tailored based on stakeholders' gaps and experiences

Figure 7: CISA cybersecurity awareness and outreach campaign to encourage public and private sector organizations and key stakeholders to take appropriate actions to "Reduce the Risk of Ransomware."

EAD Goldstein remarked, "In today's increasingly connected world, safeguarding the security and integrity of America's communications infrastructure has never been more important. CISA is dedicated to working with critical communications entities that may pose a potential national security threat to the integrity of U.S. communications networks and the communications supply chain."

EXPANDING BROADBAND ACCESS AND CONNECTION TO RURAL AND TRIBAL COMMUNITIES

May 13, 2021

Dr. Don Williams, Senior Specialist for Broadband Development, NTIA, discussed how NTIA is continuing to adapt services to meet the needs of the public, including tribal and rural communities. Current efforts include development of the National Broadband Availability Map *(Figure 8)* which includes key overlay information used to allocate grant funding, and BroadbandUSA Program's new grant programs which will allocate more than $1.5 billion to support national broadband expansion. The BroadbandUSA Program is

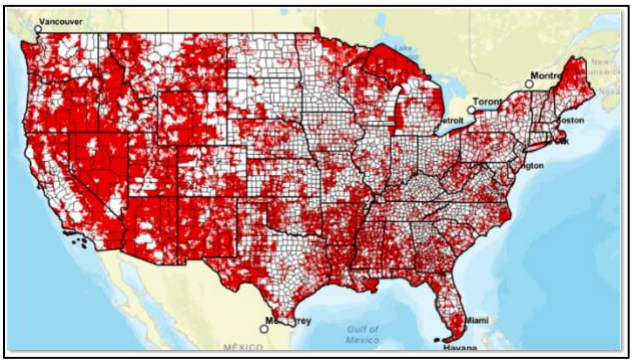

Figure 8: National Broadband Availability Map, where red areas indicate where wireline service is unavailable at the basic FCC benchmark speed of 25/3 Mbps based on FCC Form 477 data carrier-reported data.

focused on building partnerships, providing technical assistance, developing products, and hosting events to help communities become more productive and resilient.

The new BroadbandUSA grant programs are focused on supporting broadband initiatives through planning, funding, and implementation to narrow the gap and support the more than 17 million Americans who do not currently have reliable access to basic broadband services.

Dr. Williams discussed how each grant program will support investment not only in basic home access, but also support digital inclusion and literacy efforts, workforce development, and access to human services such as telehealth and education and learning programs. These grant programs will also enable and strengthen government infrastructure and resilience and enable business development to help communities grow and thrive. He also provided a technical overview of broadband basics and explained the importance of broadband in achieving the goals of each grant program.

TEXAS WINTER STORM 'URI' COMMUNICATIONS IMPACTS

May 13, 2021

The February 13-17, 2021, winter storm presented widespread impacts across Texas including massive power outages and frigid temperatures. Power grids were unable to sustain the higher-than normal energy heating demands, and the massive storm impacted all of Texas' 254 counties. Karla Jurrens, Texas Deputy SWIC, provided insight into how Texas handled this massive storm and shared lessons learned including the essential usage of COOPs to guide response efforts and ensuring SOPs remain current and up to date.

Figure 9: 643-foot tower in Notrees, Texas, damaged by winter storm Uri.

The FCC recently updated its network outage reporting rules, specifically how information reported through the Network Outage Reporting System (NORS) and its voluntary Disaster Information Reporting System (DIRS) is shared with other partners and stakeholders. Previously, this data was only shared with the Department of Homeland Security; however, next year, the new rules will allow for increased information sharing and awareness to help states and localities respond to these types of storms and to prioritize their resources to adequately recover from their impacts. Julia Tu, FCC, provided an overview of NORS and DIRS and highlighted the federal coordination efforts during winter storm Uri. There is no cost to activate DIRS; however, doing so involves coordination between CISA Central emergency response operations, the FCC, and FEMA. Jim Lundsted, CISA Emergency Communications Coordinator for Regions 6 and 7, provided insight as to how federal coordination resources like DIRS and Emergency Support Functions (ESF), specifically ESF-2, can help states and territories.

COLLABORATING ON MUTUAL AID FOR LTE MISSION CRITICAL PUSH-TO-TALK

May 13, 2021

FirstNet Authority

Jacque Waring, Public Safety Engagement Manager, and Kim Coleman, Senior Public Safety Advisor, spoke about current FirstNet Authority activities and the momentum among public safety agencies and organizations subscribing to FirstNet services. Ms. Waring stated there is

opportunity for growth and expansion for deploying FirstNet-ready devices and assets, and they are reaching Band 14 coverage completion. Ms. Waring reiterated that FirstNet's vision is to ensure that broadband meets the needs of public safety by providing a planned and funded solution across multiple technologies. She also provided an overview of how the FirstNet Authority monitors AT&T's performance through deliverables, contract oversight, program management, and external entities who perform regular audits.

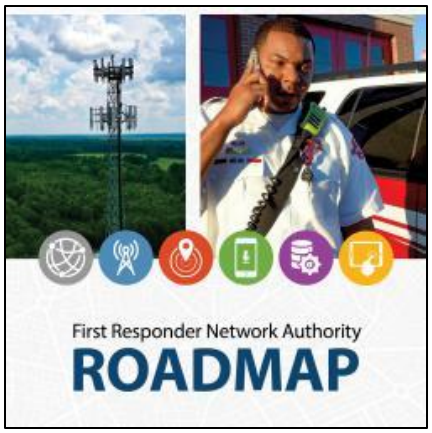

Figure 10: FirstNet Authority Roadmap

The FirstNet Authority focused on stakeholder engagement with public safety, industry, and partner organizations to guide development of the FirstNet Authority Roadmap (Figure 10), which outlines the FirstNet Authority's six domains. These domains represent the network capabilities that are vital to public safety operations and help the FirstNet Authority prioritize its programs, resources, investments, and partnership activities. These six domains include the Core central switching and connectivity system; coverage; situational awareness; voice communications; secure information exchange where Identity, Credential, and Access Management (ICAM) is managed; and user experience.

Ms. Waring stated that their current Roadmap focus is on operationalizing voice communications, with a specific focus on the development of a governance structure and policies and standards for FirstNet PTT technology. FirstNet's PTT is based on 3GPP mobile broadband standards and is currently the only PTT solution integrated into their network. FirstNet does not view PTT as a replacement for LMR, but instead sees it as augmenting LMR communications.

Ms. Coleman provided an overview and discussion of the critical need to develop a framework for mutual aid PTT in coordination with the public safety community. During a multi-agency response, first responders arriving on-scene from various jurisdictions would require immediate communications with fellow responders. There is currently no mutual-aid framework for public safety to use when adopting and operationalizing critical voice communications over LTE or FirstNet.

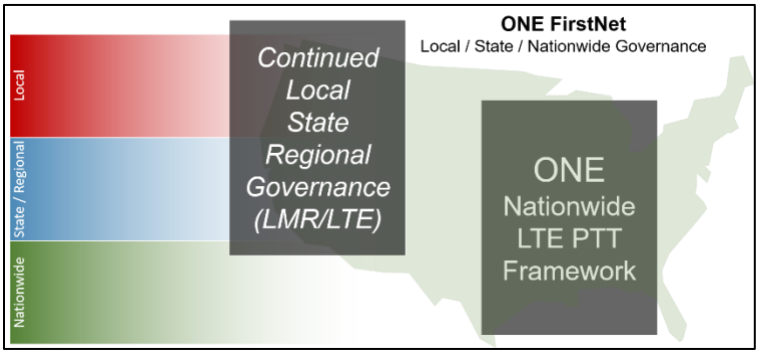

Figure 11: FirstNet envisions a standardized ONE FirstNet approach to achieving interoperable mutual aid PTT communications which will augment LMR.

LMR has a well-developed and established interoperability governance framework at the state, local, and nationwide levels. The FirstNet Authority envisions ONE FirstNet approach to developing a similar framework to support interoperable communications across LTE PTT. This framework would address the organization and governance of talk groups to enable federal and SLTT first responder agencies to communicate efficiently and effectively during joint response efforts. Governance of these talk groups would include standardized naming conventions developed in coordination with SAFECOM and NCSWIC.

ACCESS VIRTUAL ENGAGEMENT SESSION RECORDINGS!

Please contact the SAFECOM Inbox or NCSWIC Inbox with questions or feedback.