SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) conducted a virtual roundtable. Members shared best practices and lessons learned for balancing response efforts to real-world events during the public health crisis, including natural disasters, cyber incidents, unplanned large-scale demonstrations, and planned events. Speakers discussed their experiences responding to many of the events that occurred in 2020 and highlighted key areas where they focused efforts to ensure the continuity and resiliency of their agency's public safety communications.

During the roundtable, best practices emerged as speakers noted similarities in response efforts across the country. Several of the most common factors include:

- Ensuring proper resource management
- Maintaining a healthy and robust workforce through preventive measures
- Focusing on training
- Updating or developing plans and procedures
- Ensuring resiliency and cybersecurity in a virtual environment
- Applying responsible fiscal choices due to budget limitations
- Providing accessible educational and mental health services to personnel

The graphic below, and continued on the following page, is an extensive, but not all-inclusive, snapshot of 2020 events that demonstrates the wide array of incidents impacting public safety communications and first responders. Speakers touched on a number of events to include: the tornado outbreak in Tennessee, the national health crisis, widespread civil unrest, the T-Mobile outage, Hurricane Hanna, and Tropical Storm Isaias.

SAFECOM and NCSWIC will continue to share best practices and lessons learned during future webinars with topics including encryption and establishing a virtual emergency operations center (EOC).
PLANNING
• Develop scalable local, statewide, and regional emergency communications plans that include procedures for shared information and resources to support operable, interoperable, secure, and resilient communications
• Modify operations plans/standard operating procedures to account for social distancing regulations within temporary emergency shelters
• Pre-program talk groups into radios to support interoperability and limit time spent on reprogramming
• Review and update continuity of operations plans on a regular basis and conduct periodic training with members from all disciplines involved in emergency response to promote familiarity with the plans prior to an incident
• Leverage existing relationships with neighboring jurisdictions, partner offices, and wireless carriers, and foster new relationships with non-traditional partners

TRAINING
• Utilize virtual or in-person statewide and regional technical assistance offerings from the Cybersecurity and Infrastructure Security Agency (CISA), to keep up-to-date with new technologies, enhance governance policies, and manage Communications Unit (COMU) resources
• Ensure all relevant staff are functioning under the same operational framework, response approach, and procedural guidance, such as the National Incident Management System Incident Command Structure for consistent response management
• Encourage personnel to take advantage of the expanded availability of COMU trainings and emphasize the importance of such trainings

PERSONNEL
• Promote staff health and safety by implementing preventive measures (e.g., encouraging hand washing and providing access to hand sanitizer) and establishing safety protocols (e.g., temperature checks, medical screening questionnaires)
• Explore telework and other remote work options to limit potential exposure to and transmission of a virus
• Provide accessible educational and mental health services to personnel and their families
• Utilize an internal coordination group to help manage staffing and testing of exposed staff, and ensure the availability of adequate testing resources based on response staffing requirements

CYBERSECURITY
• Remain vigilant and up-to-date on the latest cyber vulnerabilities by subscribing to alerts, bulletins, and reports available from CISA’s National Cyber Awareness System
• Utilize the CISA Services Catalog, a list of risk management and response services, to build resiliency and form partnerships encouraging information sharing and promote the protection of physical and digital systems
• Implement proven protocols for teleworking (e.g., CISA Telework Guidance) to lessen potential points of intrusion
• Evaluate current communications and cybersecurity resiliency capabilities (e.g., CISA’s Public Safety Communications and Cyber Resiliency Toolkit) and implement mitigation strategies to address identified vulnerabilities
• Work with commercial network providers and CISA’s Priority Telecommunications Services to ensure priority internet and voice connections to support emergency response efforts

RESOURCES
• Establish protocols to transfer calls for service from public safety answering points temporarily closed (e.g., for cleaning due to illness or quarantine; power outages)
• Maintain an adequate stockpile of resources (e.g., consumable resources to include personal protective equipment, cleaning supplies, and batteries; extra/replacement equipment) as availability and accessibility may be limited during an emergency