



2020

ANNUAL SUMMARY

*A summary of key products, activities,
and major meeting outcomes in 2020*



Contents

INTRODUCTION	2
2020 IMPACT ON PUBLIC SAFETY COMMUNICATIONS	2
EXECUTIVE BOARD	2
EDUCATION AND OUTREACH COMMITTEE	3
GOVERNANCE COMMITTEE	3
FUNDING AND SUSTAINMENT COMMITTEE	4
TECHNOLOGY POLICY COMMITTEE	5
COMMUNICATIONS SECTION TASK FORCE	6
INFORMATION SHARING FRAMEWORK TASK FORCE	7
PROJECT 25 COMPLIANCE ASSESSMENT PROGRAM TASK FORCE	7
2020 VIRTUAL MEETINGS	7
SAFECOM at External Conferences	7
CISA Support During the Health Crisis Webinar (May 15)	8
Cybersecurity 101 Webinar (May 29)	8
Preparing for 2020 Real-World Events Webinar: Lessons Learned for Public Safety Communications (August 12)	9
Virtual Emergency Operations Centers Webinar: Lessons Learned from Hurricane Isaias (October 1)	11
Fall 2020 Virtual Engagement (December 1-3; 8-10)	11
SAFECOM'S CONTRIBUTIONS TO NATIONWIDE GUIDANCE	11
2020 SAFECOM ELECTIONS	11
2020 NEW MEMBERSHIP	12

VISION

Assuring a safer America through effective public safety communications

MISSION

SAFECOM, as an advisory body to the Department of Homeland Security (DHS), improves public safety communications operability, interoperability, and security across local, regional, state, tribal, territorial, and international borders, and with Federal Government entities

INTRODUCTION

In 2020, SAFECOM, administered by the Cybersecurity and Infrastructure Security Agency (CISA)¹ and led by the SAFECOM Executive Board, worked to enhance public safety communications capabilities and improve coordination among the community. SAFECOM supported the progress of strategic priorities through its four committees: Education and Outreach, Governance, Funding and Sustainment,² and Technology Policy.³ Additionally, SAFECOM members supported a number of other initiatives through organized task forces and working groups comprised of SAFECOM members and subject matter experts across multiple disciplines and levels of government, with an emphasis on revising the [SAFECOM Interoperability Continuum](#); enhancing SAFECOM’s membership; identifying cybersecurity risks relevant to public safety communications; supporting the transition to Next Generation 911 (NG911); providing user input to Project 25 (P25) standards and compliance; revising the communications structure of the National Incident Management System (NIMS) Incident Command System (ICS); and creating an Information Sharing Framework (ISF). This document provides a summary of key 2020 SAFECOM products and activities, as well as summaries of virtual meetings conducted throughout the year.

2020 IMPACT ON PUBLIC SAFETY COMMUNICATIONS

EXECUTIVE BOARD

The Executive Board is comprised of an 11-member board, which includes the SAFECOM Chair, First and Second Vice Chairs, each of the four committee chairs, and four additional board members. The Board serves as the program’s leadership group and provides strategic guidance to SAFECOM on emergency responder user needs. The Board is also responsible for maintaining programmatic resources, including the *SAFECOM Strategic Plan* and the *SAFECOM Annual Summary*. The Strategic Plan outlines the function of SAFECOM and its sub-groups’ current year planned priorities, products, and activities. The Annual Summary highlights SAFECOM’s previous year accomplishments and activities.

Executive Board Accomplishments

- Chair:** Chief Gerald Reardon
- First Vice Chair:** Deputy Chief Chris Lombard
- Second Vice Chair:** Michael Murphy (November 2017 – December 2020); Chief Jay Kopstein (December 2020 – Current)
- ✓ [2019 SAFECOM Annual Summary](#)
- ✓ [2020 SAFECOM Strategic Plan](#)

¹ 6 U.S. Code Section 571 (c) (2) requires CISA to administer the Department’s responsibilities and authorities relating to the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards

² Jointly coordinated with the National Council of Statewide Interoperability Coordinators (NCSWIC)

³ Jointly coordinated with NCSWIC

EDUCATION AND OUTREACH COMMITTEE

The Education and Outreach Committee continued to promote SAFECOM's role and its impact on public safety communications nationwide through participation at public safety incidents and virtual events, and through the publication of blog posts and website updates. The Committee hosted a SAFECOM School and New Member Webinar in November 2020 as an opportunity for new members to learn more about the SAFECOM Program, membership requirements and expectations, and the importance of active participation. In addition to strategizing methods and platforms to best communicate SAFECOM's mission, goals, and priorities, the Committee also published *Succession Planning Resources for Public Safety Communications: A Planning and Program Guide for Public Safety Communications Personnel*. The document recommends public safety agencies identify public safety communications coordinators and provides an overview of how public safety organizations can retain institutional knowledge through transitioning traditional public safety into communications roles. To measure SAFECOM's impact in the public safety community, the Committee also developed the *SAFECOM Outreach and Engagement Bi-Annual Report*, which summarizes and analyzes the impacts of SAFECOM's outreach and engagement activities from July to December of 2019.

Education and Outreach Committee Accomplishments

Chair: Michael Davis
Vice Chair: Sean Fensterwald

- ✓ [Blog Posts](#)
- ✓ SAFECOM School and New Member Webinar
- ✓ [Succession Planning Resources for Public Safety Communications: A Planning and Program Guide for Public Safety Communications Personnel](#)
- ✓ *SAFECOM Outreach and Engagement Bi-Annual Report*

Interoperability Continuum Working Group Accomplishments

Chair: Chief Jay Kopstein

- ✓ [SAFECOM Interoperability Continuum](#) Graphic and Brochure Update
- ✓ Supplementary [Frequently Asked Questions](#) Document

Interoperability Continuum Working Group: The Interoperability Continuum Working Group was charged with updating the *SAFECOM Interoperability Continuum*⁴ brochure and developing recommendations and best practices based on the core objectives in the Continuum. The Working Group completed updates to the *Interoperability Continuum* and developed supplementary documentation to answer any questions from the public safety community. Highlights of the

updates include an added focus on information and cyber security, as well as an expansion of the governance section to address lifecycle funding. The updated *Interoperability Continuum* and its supporting documents were [published in June 2021](#).

GOVERNANCE COMMITTEE

The Governance Committee focused on improving governance structures and processes internal to SAFECOM. The Governance Committee oversaw the management of SAFECOM's membership through its annual membership assessment to determine potential gaps in membership. The Membership Working Group reviewed membership applications received and provided recommendations to the Executive Board for new membership. The Committee also led efforts to revise and update the *SAFECOM Governance Charter*, in coordination with CISA and the Executive Board.

Governance Committee Accomplishments

Chair: Captain George Perera
Vice Chair: Sheriff Paul Fitzgerald

- ✓ Annual Membership Assessment Process
- ✓ Recommendations for New SAFECOM Membership

Cybersecurity Working Group: The Cybersecurity Working Group shares actionable guidance and informational materials with peers regarding cybersecurity risks relevant to public safety communications. The Working Group shares planning and mitigation guidance regarding known threats and vulnerabilities to public safety communications; consolidates and publishes information on cybersecurity services and grant programs; and works collaboratively with other groups to develop and share information on equipment and protocol vulnerabilities impacting the public safety mission.

⁴ Work towards updating the *Continuum* contributes to *National Emergency Communications Plan* (NECP) Objective 6.3; Success Indicator: SAFECOM updates the *Interoperability Continuum* to account for cybersecurity. August 2021

Cybersecurity Working Group Accomplishments

Chair: Mark Hogan

Vice Chair: Captain George Perera

- ✓ [Cyber Risks to Public Safety: Ransomware Guide](#)
- ✓ Distributed Cybersecurity Guidance to Stakeholders and Reinforced Critical Alerts
 - [CISA Cyber Essentials Toolkit](#)
 - [CISA Insights: Ransomware Outbreak](#)
 - US-CERT Alert: [Technical Approaches to Uncovering and Remediating Malicious Activity](#)
 - Security Updates for Critical Product Vulnerabilities (Adobe, Cisco, Google)
 - [November 2020 Microsoft Security Updates](#)
 - [December 2020 Microsoft Security Updates](#)

In 2020, the Working Group⁵ identified issues pertinent to the public safety community, such as ransomware, encryption, cybersecurity incident response, cybersecurity insurance, and cybersecurity risks to land mobile radio (LMR), and shared personal planning experiences on how to respond to ransomware and other cyber incidents and insights into purchasing cybersecurity insurance. Additionally, the group received presentations from experts, including on common cyberattacks against public safety answering points; distributed timely guidance, such as informational messaging on the release of CISA's *Cyber Essential* chapters and *CISA Insights*; and reinforced critical alerts from the United States Computer Emergency Readiness Team (US-CERT) and other CISA alerts pertinent to public safety. The Working Group also provided feedback and assisted with the publication of the *CISA Cyber Risks to Public Safety: Ransomware* guide.

FUNDING AND SUSTAINMENT COMMITTEE

The Funding and Sustainment Committee continued to identify innovative funding and sustainment solutions, disseminate information on available funding opportunities, and inform stakeholders on key issues impacting public safety communications budgets. To help agencies determine appropriate solutions that strike a balance between cost and value, the Committee first developed the *Emergency Communications Systems Value Analysis Guide*.⁶ The Guide compiles recommendations, best practices, and considerations for public safety agencies to evaluate cost effectiveness. The accompanying brochure, *Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers*, provides key considerations and trade-offs between the cost and value of communications systems components, helping agencies to save money and advocate for necessary funding.

As in previous years, members also collaborated with CISA to develop the annual *SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*.⁷ The input and expertise from the Committee ensured the *SAFECOM Guidance* provided current information on emergency communications policies, eligible costs, best practices, and technical standards for state, local, tribal, and territorial (SLTT) grant recipients investing federal funds in emergency communications projects.

Additionally, the Funding and Sustainment Committee provided a quick and comprehensive analysis of the [Coronavirus Aid, Relief, and Economic Security \(CARES\) Act](#). Released internally to SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) members, the document provided information on CARES Act grants and programs relevant to public safety communications.

Funding and Sustainment Committee Accomplishments

SAFECOM Chair: Lloyd Mitchell

Vice Chair: Chief Bill Bamattre

- ✓ [Emergency Communications Systems Value Analysis Guide](#) and Talking Points
- ✓ [Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers](#)
- ✓ Contributed to the [SAFECOM Guidance on Emergency Communications Grants](#)
- ✓ [SAFECOM and NCSWIC Guidance on CARES Act Grants](#)

⁵ Efforts undertaken by the Working Group directly contribute to NECP Objective 2.1; Success Indicator: Public safety organizations use strategic implementation plans (e.g., Statewide Communication Interoperability Plans, Regional Interoperability Communications Plans, Next Generation 911 Plans, and cybersecurity plans) to measure progress against NECP objectives and any additional state or territory objectives, and update plans annually.

⁶ Publication of this guidance directly contributed to NECP Objective 5.3; Success Indicator: Public safety organizations follow acquisition best practices, including consideration for standards-based infrastructure.

⁷ Publication of this guidance directly contributed to NECP Objective 1.2; Success Indicator: Governance bodies coordinate with elected officials to champion public safety communications priorities and lifecycle planning among decision makers.

TECHNOLOGY POLICY COMMITTEE

The Technology Policy Committee continued to promote the use of technologies, resources, and processes related to emergency communications and interoperability in coordination with SAFECOM and NCSWIC members. The Technology Policy Committee continued to support LMR systems, promote broadband technology and deployment, encourage public safety information sharing, and work with all government partners to further the use and security of various technologies within the emergency communications ecosystem⁸—Identity, Credential, and Access Management (ICAM), NG911, advanced technologies, and cybersecurity.

The Committee released several products in 2020. The *SAFECOM-NCSWIC Radio Frequency (RF) Interference Best Practices Guidebook* summarizes active and passive sources of RF interference (“jamming”) and outlined several best practices to prevent or mitigate jamming of RF resources. The *Essentials of Alerts, Warnings, and Notifications (AWN)* outlines the fundamentals of AWN systems and the evolving AWN landscape, future considerations, and examples of existing systems. The *Best Practices for Planning and Implementation of P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI): Volume II*⁹ describes technology, stakeholders, and long-term planning elements of P25 ISSI/CSSI implementation. The *Encryption Key Management Fact Sheet* and *Operational Best Practices for Encryption Key*

Management summarize encryption key management and provide several best practices and recommendations at the operational level to optimally manage the use of encryption and encryption keys. The *ICAM Value Proposition Suite* underscores the value of Federated ICAM in responding to four emergency response scenarios: hurricanes, drug epidemics, school shootings, and serial bombings. The *Public Safety Communications Dependencies on Non-Agency Infrastructure and Services*¹⁰ describes communications dependencies on third-party providers for infrastructure or services, the challenges associated with such dependencies, and best practices to mitigate or prevent system downtime due to dependencies outages or failures.

Technology Policy Committee Accomplishments

Chair: Phil Mann

- ✓ [SAFECOM-NCSWIC RF Interference Best Practices Guidebook](#)
- ✓ [Essentials of AWN](#)
- ✓ [Best Practices for Planning and Implementation of P25 ISSI and CSSI: Volume II](#)
- ✓ [ICAM Value Proposition Suite](#)
- ✓ [Encryption Key Management Fact Sheet](#)
- ✓ [Operational Best Practices for Encryption Key Management](#)
- ✓ [Public Safety Communications Dependencies on Non-Agency Infrastructure and Services](#)

NG911 Working Group Accomplishments

Chair: Mark Buchholz

Vice Chair: Jeremy DeMar

- ✓ [NG911 Self-Assessment Tool](#)
- ✓ National 911 Program’s [State of 911 Webinar Series](#)
- ✓ [Cyber Risks to NG911](#) White Paper
- ✓ Cyber Threats to 911 Centers’ Presentation at the IACP Virtual Conference and Expo
- ✓ [GIS Lifecycle Best Practices Guide for NG911](#)

NG911 Working Group: The NG911 Working Group¹¹ utilizes stakeholder feedback from multiple levels of government to identify short- and long-term priorities which will support efforts to fund, assess readiness, and complete the transition to NG911. In 2020, the Working Group promoted the *NG911 Self-Assessment Tool*, published on [911.gov](#). The Tool helps 911 center administrators and oversight personnel evaluate a system’s NG911 maturity state and understand the next steps necessary to continue the NG911 deployment progress. In January 2020, the Working Group presented on the National 911 Program’s *State of 911 Webinar Series* to raise

awareness about the Tool within the 911 community. To promote cybersecurity for NG911 systems, the Working Group published an update to the *Cyber Risks to NG911* white paper, which provides an overview of the cyber risks

⁸ Efforts undertaken by the Committee directly contribute to NECP Objective 5.2; Success Indicator: SAFECOM and the NCSWIC communicate emerging technology impacts to public safety, such as those associated with identity management, multimedia, 5G, Internet of Things, social media, network virtualization, spectrum optimization, artificial intelligence, machine intelligence, geographic information systems, and positioning, navigation, and timing systems.

⁹ Publication of this guidance directly contributed to NECP Objective 5.2; Success Indicator: SAFECOM and the NCSWIC guide standards-based LMR evolution.

¹⁰ Publication of this guidance directly contributed to NECP Objective 4.2; Success Indicator: Public safety organizations periodically evaluate, engage, and incorporate commercial and non-traditional communications partners (e.g., auxiliary communications, volunteers, and utilities) in incidents and planned events.

¹¹ Efforts undertaken by the Working Group directly contribute to NECP Objective 5.2; Success Indicator: The National 911 Program coordinates, in collaboration with all levels of government, the optimization of 911 services, including the Nation’s transition to NG911.

that will be faced by NG911 systems, mitigation strategies, and education and training resources. The group also presented on cyber threats to 911 centers at the International Association of Chiefs of Police (IACP) Virtual Conference and Expo. The presentation provided public safety stakeholders with actionable steps to enhance the cybersecurity posture of NG911 systems and highlighted SAFECOM, NCSWIC, and CISA cybersecurity resources.

To support stakeholders in the transition to NG911, the Working Group published the *Geographical Information Systems (GIS) Lifecycle Best Practices Guide for NG911*, which provides an overview of the GIS lifecycle, best practices for each phase of the lifecycle, and resources for GIS support, along with a companion document, *California Statewide NG911 GIS Use Case* (publication expected early 2021). Public safety administrators, managers, and officials can use this document to familiarize themselves with GIS lifecycle best practices to ensure they have implemented essential GIS components for NG911.

P25 User Needs Working Group: The P25 User Needs Working Group (UNWG) is a forum in which a broad range of public safety users and user representatives may provide user input into the P25 standards development process. In 2020, the P25 UNWG established the Global Positioning System (GPS) Focus Group to gather input from users on their current and planned uses of GPS in their LMR systems to develop a formal recommendation for consideration by the P25 Steering Committee¹² into the P25 standards development to comply with the Natural Resources Management Act.

P25 UNWG Accomplishment
SAFECOM Co-Chair: Scott Wright
✓ GPS Focus Group Establishment

COMMUNICATIONS SECTION TASK FORCE

The Communications Section Task Force (CSTF)¹³ addresses challenges associated with supporting information and communications technology (ICT) within the NIMS ICS. The CSTF continues to work towards developing a nationwide federated governance framework through the Incident Communications Advisory Council, a focus group created to review and validate the CSTF’s recommendations for enhancing the functionality of NIMS.

In January 2020, CISA presented the CSTF’s NIMS ICS Refresh Recommendation to the Federal Emergency Management Agency (FEMA) Administrator to propose a series of updates to better align NIMS ICS with the changing communications environment. These recommendations included creating new positions and modernizing the ICS structure. Throughout the remainder of 2020, CISA and the CSTF participated in the FEMA National Integration Center (NIC) Coordination Group Communications and Technology Sub-Groups to continue engaging with FEMA NIC and its stakeholders to reinforce the need for modifying NIMS ICS to better manage incident ICT. The Task Force also engaged with stakeholders during its communications incident management presentation at the International Wireless Communications Expo’s (IWCE) virtual conference in August 2020.

Additionally, the CSTF assisted the CISA Interoperable Communications Technical Assistance Program (ICTAP) subdivision with revising the Information Technology Service Unit Leader (ITSL) curriculum. Units 1-15 were revised based on instructor and participant feedback. The completed ITSL Refresh is expected to be finalized in Spring 2021. Finally, the CSTF developed an *ICT Recruitment and Retention Plan* to serve as a strategic plan for recruiting, training, supporting, and retaining a pool of candidates to support information and communications management at planned events or incidents.

CSTF Accomplishments
Chair: Deputy Chief Chris Lombard
Vice Chair: John Miller
✓ NIMS ICS Refresh Recommendation
✓ FEMA NIC Re-engagement Plan
✓ Communications Incident Management Presentation to IWCE
✓ ITSL Refresh (Ongoing)
✓ ICT Recruitment and Retention Plan

¹² The P25 Steering Committee is an independent body comprised of representatives from a range of organizations at all levels of public safety.

¹³ Efforts undertaken by the Task Force directly contribute to NECP Objective 3.1; Success Indicator: Public safety organizations coordinate training and technical assistance across levels of government (as applicable) to ensure current and consistent information; and NECP Objective 3.3; Success Indicator: SAFECOM and the NCSWIC develop training curriculums for additional positions within the Information Technology Service Unit.

INFORMATION SHARING FRAMEWORK TASK FORCE

Established in conjunction with NCSWIC, the Information Sharing Framework Task Force (ISFTF)¹⁴ continued to develop a data interoperability framework, expanding beyond the current “single organization” information sharing. The ISFTF also develops technical/operational standards to enable secure information flow between disparate public safety systems and defines best practices for data/icon security and interoperability in an Internet Protocol environment based on standards and/or other solutions leveraging new “big data” players. In 2020, the ISFTF developed a final specification for the ISF structure, an example of ISF customization via a National Public Safety Telecommunications Council use case; further developed Appendices A (Baseline Technological Assessment), B (Use Cases), and C (Regulatory, Legal, Contractual, and Financial Considerations); and assessed existing data exchange/information sharing documents for synergies, including the NG911 Standards Compendium used for NG911 Cost Study and the Information Sharing Assessment Tool. Additionally, the ISFTF helped SAFECOM grant applicants with data exchange and information sharing solutions evaluation.

ISFTF Accomplishments

Chair: Sheriff Paul Fitzgerald

- ✓ ISF Revision 2.0
- ✓ SAFECOM *Guidance on Emergency Communications Grants for Fiscal Year 2021* Submission for Appendix B – Technology and Equipment Standards and Resources

P25 COMPLIANCE ASSESSMENT PROGRAM TASK FORCE

In coordination with NCSWIC, the P25 Compliance Assessment Program Task Force (CAPTF)¹⁵ provides public safety community input into the DHS P25 CAP, which assesses compliance of communications equipment to the P25 Suite of Standards. In 2020, the P25 CAPTF reviewed and provided input on the *ISSI/CSSI Conformance Test Tool Compliance Assessment Bulletin (ICC Test Tool CAB)* developed by the DHS Science and Technology Directorate (S&T). The document provides the verification procedures for test tool products that are designed to perform conformance testing of P25 ISSI and CSSI equipment in accordance with P25 CAP ISSI and CSSI Conformance Test Cases and Pass/Fail documents, creating a robust and repeatable verification program in accordance with applicable DHS S&T and P25 CAP technical and reporting requirements.

P25 CAPTF Accomplishments

Chair: Chief Gerald Reardon

- ✓ ICC Test Tool CAB Input

2020 VIRTUAL MEETINGS

Due to travel restrictions throughout 2020, the traditional in-person meetings hosted by CISA were held virtually. Regardless, this series of virtual meetings continued to promote collaboration and networking among stakeholders, as well as facilitated solutions to some of the nation’s most pressing issues on emergency communications interoperability. Below are summaries of the larger virtual meetings. Full summaries for these virtual meetings and other in-person meetings may be found under the *Joint Meetings* section of the [SAFECOM website](#). In addition to these larger virtual meetings, SAFECOM’s sub-groups also met virtually throughout the year. Across 14 sub-groups, SAFECOM held a total of 93 committee, working group, and task force meetings in 2020—with 1 Executive Board meeting held in person before travel restrictions took effect, and 92 virtual meetings. In addition to these meetings, several of the sub-groups also presented during external conferences (see the box to the right).

SAFECOM AT EXTERNAL CONFERENCES

The NG911 Working Group presented virtually during the National 911 Program’s State of 911 webinar series on January 14, 2020, and during the IACP Virtual Conference and Expo on October 21-23, 2020.

The CSTF also presented “Communications Incident Management” virtually at the IWCE on August 26, 2020.

¹⁴ Efforts undertaken by the Task Force directly contribute to NECP Objective 5.3; Success Indicator: SAFECOM and the NCSWIC publish best practices and updated guidance on standard operating procedures to help the public safety community overcome data storage, exchange, maintenance, and analysis challenges.

¹⁵ Efforts undertaken by the Task Force directly contribute to NECP Objective 5.2; Success Indicator: SAFECOM and the NCSWIC guide standards-based LMR evolution.

CISA SUPPORT DURING THE HEALTH CRISIS WEBINAR (MAY 15)

Former CISA Deputy Director, Matthew Travis, provided opening remarks to kick off the first in a series of joint SAFECOM and NCSWIC webinars. Deputy Director Travis emphasized CISA's continued support of public safety stakeholders during and after the pandemic by utilizing a variety of virtual engagements including presentations, trainings, and forums for sharing best practices and lessons learned. The NCSWIC Co-Chairs of the joint SAFECOM-NCSWIC Funding and Sustainment Committee provided state perspectives on impacts of the ongoing pandemic, including balancing an increased need for resources during a time of decreased revenue and budget cuts. CISA showcased its yearly publication of the [SAFECOM Guidance on Emergency Communications Grants](#) and provided information on the regularly-updated [List of Federal Financial Assistance Programs Funding Emergency Communications](#). Additionally, CISA published guidance on the [CARES Act](#) released on March 27, 2020. Members also received an overview of the Priority Telecommunications Services offered by CISA, including Government Emergency Telecommunications Service, Wireless Priority Services, and Telecommunications Service Priority. CISA's priority services programs provided additional direct support during the pandemic, including facilitating virtual private network access to United States Navy ships utilized as alternate care sites (ACS), assisting 3M in expediting communications to support the manufacturing of personal protective equipment, and supporting medical research and testing at Walter Reed National Military Medical Center.

To assist states, territories, and tribes during this time, the CISA ICTAP subdivision shifted its focus to transitioning several of its technical assistance offerings to a virtual format. ICTAP also provided support to stakeholders on the front lines through direct support by CISA Emergency Communications Coordinators (ECC) on Emergency Support Function #2 task forces in Regions, I, II, and IX. Specific to the pandemic, ECCs actively monitored public safety answering point call volume and supported the deployment and decommissioning of ACS. Other efforts included supporting the Democratic and Republican National Conventions and Presidential Inauguration preparation in Washington, DC.

CYBERSECURITY 101 WEBINAR (MAY 29)

The Cybersecurity 101 Webinar addressed how to create a better cybersecurity posture in agencies, cybersecurity in a pandemic environment, how to engage with CISA Regional Offices, and available CISA guidance and resources. CISA uses a regional structure to provide resources, including training and direct coordination with partners, to defend against today's threats and to build more secure and resilient infrastructure for the future. Each region is led by a regional director who oversees coordination with critical infrastructure partners, along with assigned local Protective Security Advisors (PSA), technical advisors, Cyber Security Advisors (CSA), ECCs, and other CISA support deployed into the regions.

The PSA program's mission is to proactively engage with mission partners to protect critical infrastructure. PSAs serve as critical infrastructure security specialists with a focus on building relationships and sharing information. The CSA program's mission is to promote and advance cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure and SLTT governments through stakeholder partnerships and direct assistance activities. To promote the security and resilience of critical infrastructure, the CSA program conducts assessments; promotes best practices, such as the National Institute of Standards and Technology [Cybersecurity Framework](#); builds communities of interest; shares trends and security practices; listens to stakeholders and collects requirements for CISA action; and coordinates incident response.

[Federal Virtual Training Environment](#) (FedVTE) is a free online, on-demand cybersecurity training system available at no charge for government personnel, including contractors and veterans. Managed by CISA, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. CISA designed the [Cyber Essentials](#) to enhance the Nation's collective defense against cyber threats. This resource is a starting point for small businesses and local governments that do not have abundant resources to address cybersecurity risks. These essential elements are meant to outline the actions that leaders should take to create a culture of cyber-readiness in their organization.

CISA engaged a three-pronged approach in response to the pandemic, beginning with better fortifying the defenses of health sector organizations, distributing alerts on scams related to the financial stimulus package, and

supporting and strengthening organizational telework efforts. Additionally, the Multi-State Information Sharing and Analysis Center (MS-ISAC), funded by CISA, serves as a central resource for situational awareness, information sharing, and incident response for SLTT governments. More information on joining the MS-ISAC can be found at learn.cisecurity.org/ms-isac-registration.

PREPARING FOR 2020 REAL-WORLD EVENTS WEBINAR: LESSONS LEARNED FOR PUBLIC SAFETY COMMUNICATIONS (AUGUST 12)

During this virtual roundtable, SAFECOM and NCSWIC 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. Speakers touched on a number of events including: the tornado outbreak in Tennessee, the national health crisis, widespread civil unrest, the T-Mobile outage, Hurricane Hanna, and Tropical Storm Isaias. The graphic (Figure 1) 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.

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

- 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

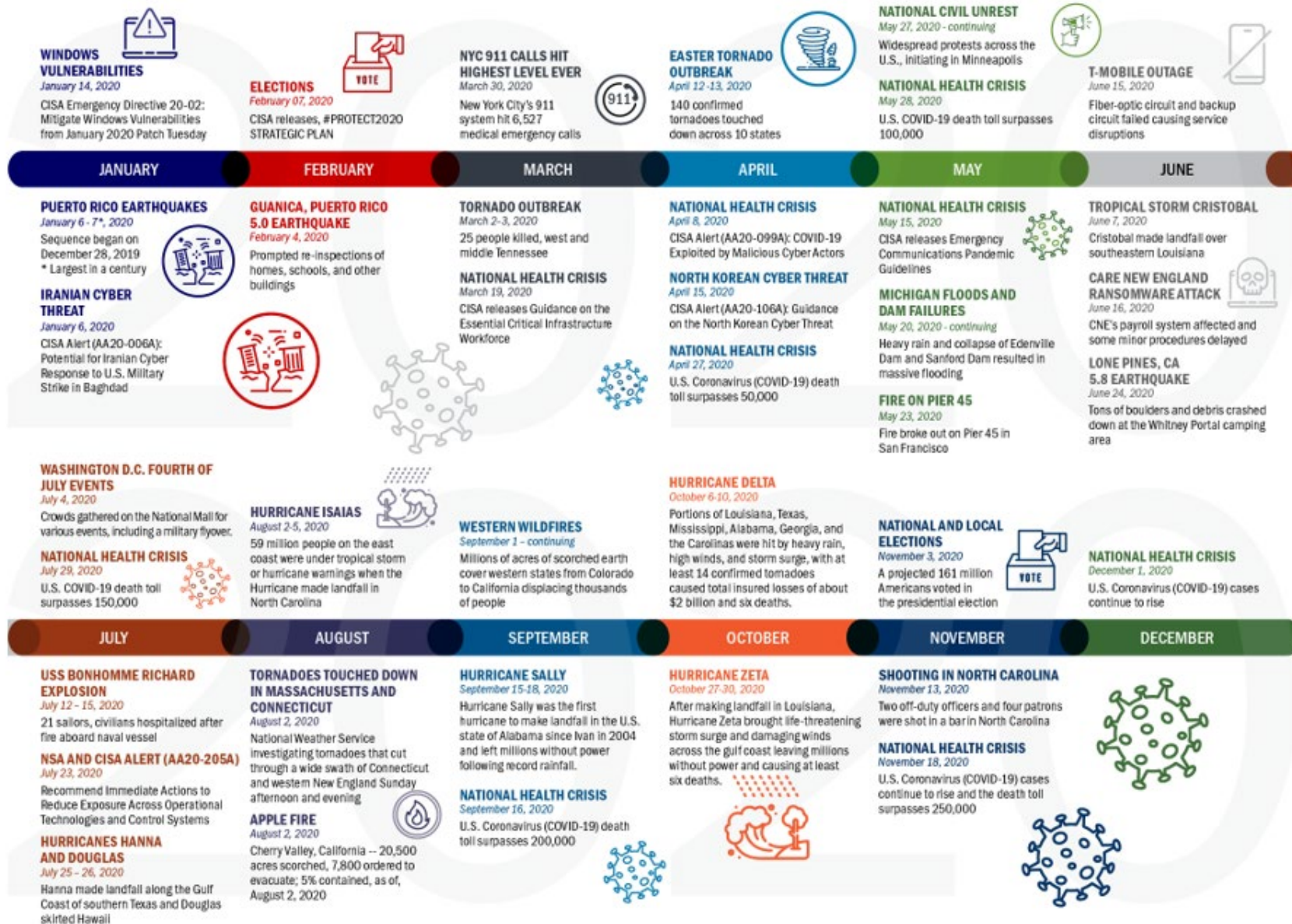


Figure 1: Snapshot of 2020 events demonstrating the wide array of incidents impacting public safety communications and first responders

VIRTUAL EMERGENCY OPERATIONS CENTERS (EOC) WEBINAR: LESSONS LEARNED FROM HURRICANE ISAIAS (OCTOBER 1)

EOCs are a critical component of incident response for planned (e.g., presidential inauguration, sporting events) or unplanned (e.g., hurricanes, wildfires, civil unrest) events. In today's environment, where social distancing requirements limit in-person interactions, the public safety community must consider options for remote coordination. Jurisdictions are now exploring the costs and benefits of augmenting traditional brick-and-mortar EOCs with a virtual environment. While most agree new digital or hybrid models will never replace face-to-face interaction during emergencies, the incorporation of a virtual EOC (vEOC) model should be considered as agencies attempt to navigate changes to the public safety communications ecosystem prompted by the pandemic.

During the webinar, participants heard from NCSWIC members and colleagues from North and South Carolina who shared their experiences implementing a vEOC in response to Hurricane Isaias and subsequent planned events. Speakers also shared best practices and highlighted digital platforms utilized in their virtually coordinated response activities, including WebEx, Bridge 4 Public Safety, Adobe Connect, and SharePoint. Visit the [full summary](#) to view a checklist for implementing a vEOC, complete with unique considerations an agency should review.

FALL 2020 VIRTUAL ENGAGEMENT (DECEMBER 1-3; 8-10)

SAFECOM and NCSWIC kicked off their bi-annual meeting, conducted virtually for the first time, with multiple informative and productive sessions over the course of a two-week period. CISA Acting Director Brandon Wales served as the keynote speaker, helping to kick off the event and providing opening remarks and CISA updates.

Members of both organizations selected topics for the engagement series, focusing on the groups' most pressing priorities. Session topics included public safety cybersecurity awareness, complicating factors impacting communications response to the 2020 fire season, communications challenges and strategies surrounding the presidential inauguration, computer-aided dispatch system interoperability, and more. Both groups also met individually to discuss and vote on current work products and conduct strategic planning for 2021 activities.

View the [full summary](#) on SAFECOM's website. Virtual engagement session recordings are available to SAFECOM and NCSWIC members through the Homeland Security Information Network (HSIN).

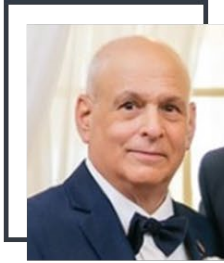
SAFECOM'S CONTRIBUTIONS TO NATIONWIDE GUIDANCE

SAFECOM members provided significant input into the [updated National Emergency Communications Plan \(NECP\)](#). Endorsed by SAFECOM, CISA released the *NECP* on September 25, 2019. The updated plan addresses current gaps within emergency communications, reflects new and emerging technological advancements, and provides guidance to drive the Nation towards a common end-state of emergency communications. SAFECOM incorporated the Plan's Success Indicators and implementation activities into its annual strategic planning and product development.

SAFECOM members also provided input for the development of [Fiscal Year 2021 SAFECOM Guidance on Emergency Communications Grants](#). Updated annually, this guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for SLTT grant recipients investing federal funds in emergency communications projects.

2020 SAFECOM ELECTIONS

In 2020, SAFECOM conducted elections for the SAFECOM Second Vice Chair, as well as leadership for the Governance and Technology Policy committees. Leadership for both committees remain unchanged, while Chief Jay Kopstein, SAFECOM At-Large, New York State Division of Homeland Security & Emergency Services, assumed the role of SAFECOM Second Vice Chair.



Chief Jay Kopstein
SAFECOM Second Vice Chair



Captain George Perera
Governance Committee Chair



Sheriff Paul Fitzgerald
Governance Committee
Vice Chair



Philip Mann
Technology Policy Committee
Chair

2020 NEW MEMBERSHIP

Each year, the Governance Committee, through the Membership Working Group, is tasked with reviewing SAFECOM's current membership for gaps in public safety disciplines and expertise. After performing an analysis of SAFECOM's membership composition, the Membership Working Group and Governance Committee review submitted SAFECOM [membership applications](#) and provide recommendations on new membership for Executive Board consideration.

In 2020, the following new associations and at-large members joined SAFECOM:

- **Associations**
 - National Law Enforcement Telecommunications System (Frank Minice and Bill Phillips)
- **At-Large Members**
 - Cindy Cast, SAFECOM At-Large, Miami-Dade County
 - John Wheaton, SAFECOM At-Large, Nez Perce Tribe

Additionally, several new association representatives were appointed by existing SAFECOM associations:

- Association of Public Safety Communications Officials (Jason Kern and Angela Bowen)
- National Sheriffs' Association (Sheriff Neil Miller)
- Major Cities Chiefs Association (Larry Satterwhite)
- National Association of Emergency Medical Technicians (William Tatum)

Many SAFECOM products are available on the [SAFECOM website](#).

For additional questions regarding the SAFECOM program, please contact SAFECOMGovernance@cisa.dhs.gov.



ASSURING A SAFER AMERICA THROUGH
EFFECTIVE PUBLIC SAFETY COMMUNICATIONS
