



2022 SAFECOM Annual Summary

A summary of key products, activities, and major meeting outcomes in 2022

March 2023

CONTENTS

INTRODUCTION	2
A NOTE FROM THE CHAIR	2
SUMMARY	3
2022 IMPACT ON PUBLIC SAFETY COMMUNICATIONS	4
EXECUTIVE BOARD	4
GOVERNANCE COMMITTEE	4
2022 SAFECOM Elections	4
2022 New Membership	5
<i>Cybersecurity Working Group</i>	6
EDUCATION AND OUTREACH COMMITTEE	6
FUNDING AND SUSTAINMENT COMMITTEE	7
TECHNOLOGY POLICY COMMITTEE	7
<i>P25 User Needs Working Group</i>	8
<i>NG911 Working Group</i>	8
COMMUNICATIONS SECTION TASK FORCE	9
INFORMATION SHARING FRAMEWORK TASK FORCE	10
P25 COMPLIANCE ASSESSMENT PROGRAM TASK FORCE	10
2022 MEETINGS	11
Spring 2022 Bi-Annual Meeting (June 8-9; Coronado, CA)	11
Fall 2022 Bi-Annual Meeting (December 13-14; Jacksonville, FL)	11
SAFECOM at External Conferences	12
SAFECOM'S CONTRIBUTIONS TO NATIONWIDE GUIDANCE	12
LOOKING AHEAD TO 2023	13

INTRODUCTION

In 2022, 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: Governance, Education and Outreach, 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 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; incorporating the full scope of Information and Communications Technology (ICT) services into the incident management organizational structure; and creating and piloting an Information Sharing Framework (ISF). This document summarizes key 2022 SAFECOM products, activities, and summaries of meetings conducted throughout the year.

A NOTE FROM THE CHAIR



Since SAFECOM's establishment in 2001, the communication and information management technologies used by the nation's public safety community have evolved and advanced dramatically, including video, data, internet protocol and broadband communications. The risk landscape has also become more challenging with more frequent and extreme weather events, cyberattacks, and the impacts of a global pandemic.

The heart of SAFECOM's mission is to improve public safety communications operability, interoperability, and security. As more sophisticated systems emerge, the need for operability, interoperability, and security to improve the ability of emergency responders to reduce the loss of life and property in emergency situations remains. And that is what propels SAFECOM forward, year after year.

SAFECOM is one of the first organizations to bring together representatives from public safety associations as well as emergency responders in the field. SAFECOM serves as a tremendous resource to first responders in providing key guidance to attain grant funding, improve interagency communications, and develop interjurisdictional and interagency relationships.

To that end, SAFECOM remains dedicated to maintaining awareness of emerging communications technologies, issues, and needs that affect the public safety community; collaborating across the public safety community to develop consensus-based guidance for emerging communications technologies, issues, and needs; and disseminating public safety communications guidance to stakeholders.

I encourage the public safety community to review and share [SAFECOM's resources](#), which span the spectrum of interoperability, from governance to technology to training and exercises. While great strides have been accomplished in the landscape of emergency communications, there is yet more work to be done. SAFECOM strives to be on the frontlines of the ever-evolving landscape, *assuring a safe America through effective public safety communications*.

Chief Gerald R. Reardon
SAFECOM Chair

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.

SUMMARY

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

To achieve our vision and mission in 2022, SAFECOM:



Focused on:

- Governance
- Education & Outreach
- Funding & Sustainment
- Technology Policy
- Communications Section
- Information Sharing
- Cybersecurity
- Next Generation 911
- Project 25 User Needs and Compliance



Welcomed

13

new members



Published over

35

new resources



Conducted over

75

meetings

2022 IMPACT ON PUBLIC SAFETY COMMUNICATIONS

EXECUTIVE BOARD

The Executive 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. In 2022, the Executive Board also played an integral role in helping to revise and update the *SAFECOM Governance Charter*.

Executive Board Accomplishments

- Chair:** Chief Gerald Reardon
- First Vice Chair:** Deputy Chief Chris Lombard
- Second Vice Chair:** Chief Jay Kopstein
- ✓ [2021 SAFECOM Annual Summary](#)
- ✓ [2022 SAFECOM Strategic Plan](#)

GOVERNANCE COMMITTEE

The Governance Committee focuses on public safety communications governance, which concentrates on improving both governance structures and processes internal to SAFECOM, as well as external statewide governance bodies for public safety communications. In 2022, the Committee oversaw the management of SAFECOM’s annual elections process and led efforts to revise and update the *SAFECOM Governance Charter*, and the *Operating Processes and Procedures*, in coordination with CISA and the Executive Board. Additionally, the Committee developed recommended procedures for external governance by crafting best practices for creating governance charters⁴ and best practices for analyzing governance structure membership in alignment with the evolving ecosystem.⁵ The Committee also focused on updating the *Writing Guide for Standard Operating Guidelines (SOG)*, a tool to assist local agencies and jurisdictions with developing guidelines for first responders when responding or operating during emergency events. This resource is expected to be published in 2023.

Governance Committee Accomplishments

- Chair:** Major George Perera
- Vice Chair:** Sheriff Paul Fitzgerald
- ✓ Annual SAFECOM Elections
- ✓ Annual Membership Assessment Process
- ✓ [SAFECOM Best Practices for Governance Charters](#)
- ✓ [SAFECOM Best Practices for Governance Structure Membership Analysis](#)
- ✓ [SAFECOM Governance Charter](#) and [Operating Processes and Procedures](#) Update
- ✓ SAFECOM Product Request Form
- ✓ SAFECOM Meeting Request Form

2022 SAFECOM Elections

In 2022, SAFECOM conducted elections for the SAFECOM Chair, Second Vice Chair, two Executive Board member positions, as well as leadership for the Governance and Technology Policy committees. As a result of each election section, leadership remained unchanged.

The 2022 Elections resulted in the following members filling leadership roles:

- **SAFECOM Chair:** Chief Gerald Reardon, SAFECOM At-Large (City of Cambridge Fire Department, Massachusetts)
- **SAFECOM Second Vice Chair:** Chief Jay Kopstein, SAFECOM At-Large (Division of Homeland Security and Emergency Services Communications and Interoperability Working Group, New York)
- **SAFECOM Executive Board Member:** Captain Anthony Catalanatto, SAFECOM At-Large (Division of Homeland Security and Emergency Services Communications and Interoperability Working Group, New York)
- **SAFECOM Executive Board Member:** Charlie Sasser, National Association of State Technology Directors
- **Governance Committee Chair:** Major George Perera, SAFECOM At-Large (Miami-Dade Police Department, Florida)

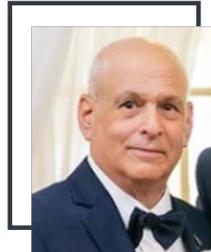
⁴ Publication of this guidance directly contributed to NECP Objective 1.1; Success Indicator: Governance bodies develop and implement governing documents, such as charters or bylaws, to clarify roles, purpose, authority, and methods for adapting to change.

⁵ Publication of this guidance directly contributed to NECP Objective 1.2; Success Indicator: Governance bodies identify and include missing or underrepresented stakeholders (e.g., jurisdictions, tribes, sectors, organizations) in formal governance structures, when developing strategic and operational plans and policies, during training and exercises.

- **Governance Committee Vice Chair:** Sheriff Paul Fitzgerald, National Sheriffs' Association
- **Technology Policy Committee Chair:** Phil Mann, American Public Works Association



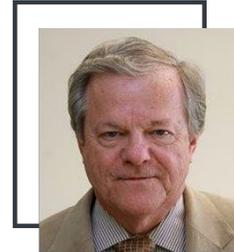
Chief Gerald Reardon (ret.)
SAFECOM Chair



Chief Jay Kopstein (ret.)
SAFECOM Second Vice Chair



Captain Anthony Catalanotto (ret.)
Executive Board Member



Charlie Sasser
Executive Board Member



Major George Perera
Governance Committee Chair



Sheriff Paul Fitzgerald
Governance Committee
Vice Chair



Phil Mann
Technology Policy
Committee Chair

2022 NEW MEMBERSHIP

Each year, the Governance Committee reviews SAFECOM's current membership for gaps in public safety disciplines and expertise. After analyzing SAFECOM's membership composition, the Governance Committee reviewed SAFECOM membership applications and provided recommendations for new members to the Executive Board.

In 2022, the following new at-large members joined SAFECOM⁶:

- Ross Bourgeois, *Director of the Real Time Crime Center for the New Orleans Office of Homeland Security and Emergency Preparedness (LA)*
- Nicole Diedrick, *Communications Bureau Administrator with the Phoenix Police Department (AZ)*
- Jonathan Goldman, *Chief, Lakes Region Mutual Fire Aid (NH)*
- Red Grasso, *FirstTech Program Director for the North Carolina Department of IT*
- Justin Kates, *Director of Emergency Management for the City of Somerville (MA)*
- Hermina "Nina" Koshinski, *Chief of Radio Operations Engineering & Support with the Pennsylvania State Police, Statewide Radio Network Division*
- Jason Trautman, *Technician, Fairfax County Fire & Rescue Department (VA)*

Additionally, several existing SAFECOM associations appointed new representatives, including:

- Charles Blankenship, *National EMS Management Association (NEMSMA) Alternate Representative*
- Jesse Cooper, *Major Cities Chiefs Association Primary Representative*
- Chief Glenn Hanson, *International Association of Chiefs of Police (IACP) Alternate Representative*
- Deputy Chief Keith Kelley, *IACP Primary Representative*
- Brooks Shannon, *National Emergency Number Association Alternate Representative*
- Dr. Hezedean Smith, *NEMSMA Primary Representative*

⁶ Based on Governance Committee membership application review, conducted in Fall 2022. New membership as of February 2023.



CYBERSECURITY WORKING GROUP: The Cybersecurity Working Group⁷ 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.

In 2022, the working group published three documents—*Cyber Risks to Land Mobile Radio (LMR): First Edition White Paper*; *“First 48”: What to Expect When a Cyber Incident Occurs*; and *Guide to Getting Started with a Cyber Risk Assessment*—and continued to share timely alerts and notifications pertinent to public safety. The group continued its mission by developing products with a focus on specific cybersecurity concerns based on membership insights and stakeholder interviews. This year, the group explored various forms of cyber risks to public safety communications, identified methods and resources to help secure these systems, and developed recommendations on how to proceed after experiencing a cyber incident in the first 48 hours. The working group also helped public safety organizations strengthen overall operational and cyber resiliency by documenting commonly-practiced risk assessment steps and identifying personnel and resources involved in a cyber risk assessment.

Cybersecurity Working Group Accomplishments

Co-Chairs: Major George Perera, Mark Hogan

- ✓ [Cyber Risks to LMR: First Edition White Paper](#)
- ✓ ["First 48": What to Expect When a Cyber Incident Occurs](#)
- ✓ [Guide to Getting Started with a Cyber Risk Assessment](#)
- ✓ Distributed five SAFECOM Cybersecurity Advisories to reinforce critical alerts:
 - State-Sponsored Exploitation of Default Multifactor Authentication Protocols
 - Microsoft Releases Advisory to Address CVE-2022-26809
 - Recent Top Routinely Exploited Vulnerabilities
 - Microsoft Releases June 2022 Security Updates
 - Microsoft Releases August 2022 Security Updates

Education and Outreach Committee Accomplishments

Chair: Michael Davis

Vice Chair: Captain Cody Worrell

- ✓ [SAFECOM Factsheet](#) Update
- ✓ [SAFECOM Membership Spotlight Series](#) (featuring Keith Victor, SAFECOM At-Large)
- ✓ [SAFECOM Membership Questionnaire](#)
- ✓ [Catching up with SAFECOM: An Education and Outreach Committee Quarterly Newsletter](#)
- ✓ SAFECOM School and New Member Orientation
- ✓ [SAFECOM Website](#) Updates

EDUCATION AND OUTREACH COMMITTEE

The Education and Outreach Committee promotes SAFECOM’s role in and impact on public safety communications nationwide through participation in public safety incidents and virtual events, as well as through blog post and website update publications. In 2022, the SAFECOM Education and Outreach Committee continued its mission to promote the vision and goals of SAFECOM by providing updates to the *SAFECOM Factsheet*. The updated *SAFECOM Factsheet* provides an overview of SAFECOM; gives a brief description of the SAFECOM membership, strategic priorities, committee structure, and public safety influence; and highlights recent

SAFECOM accomplishments. The Committee also showcased its diverse membership and collective experience with its second iteration of the *SAFECOM Membership Spotlight* featuring SAFECOM At-Large member Keith Victor (Connecticut Capitol Region of Council of Government). These Spotlights highlight the represented association or

⁷ Efforts undertaken by the Working Group directly contributed to NECP Objective 6.2; Success Indicator: SAFECOM and NCSWIC share planning and mitigation guidance regarding known threats and vulnerabilities.

organization as well as members’ unique skill sets, achievements, and education that work together to improve the public safety community.

The Committee also developed *Catching up with SAFECOM: An Education and Outreach Committee Quarterly Newsletter*. This newsletter will be distributed on a quarterly basis to SAFECOM and its affiliates via email and a web-based email subscription management system housing over 60k+ subscribers. This newsletter will educate readers on SAFECOM’s most recent publications, community actions, and upcoming public safety events where SAFECOM will be present. To better understand the make-up of SAFECOM’s membership, the Committee also developed the *SAFECOM Membership Questionnaire*. This tool is used to collect public safety experience from SAFECOM members to identify membership gaps, obtain updated information on SAFECOM’s membership body, and to assist in updating SAFECOM resources to reflect the current state of the nation’s emergency communications. The *SAFECOM Membership Questionnaire* is scheduled to be released to the full membership in spring 2023. Finally, the Committee hosted a SAFECOM School and New Member Webinar in June 2022 to provide new members with opportunities to learn more about the SAFECOM program, membership requirements and expectations, and the importance of active participation.

FUNDING AND SUSTAINMENT COMMITTEE

Throughout 2022, the Funding and Sustainment Committee,⁸ in coordination with the National Council of Statewide Interoperability Coordinators (NCSWIC), continued to create a series of products highlighting strategies for maintaining and securing funding for emergency communications projects. The Committee began the year by providing subject matter expertise on the *Fiscal Year (FY) 2022 SAFECOM Guidance on Emergency Communications Grants*, helping to make emergency communications policies, best practices, and technology standards consistent across the nation.

Funding and Sustainment Committee Accomplishments
SAFECOM Chair: Lloyd Mitchell
Vice Chair: Chief Bill Bamattre
✓ FY22 SAFECOM Guidance on Emergency Communications Grants
✓ Contingency Planning Guide for Emergency Communications Funding
✓ Contingency Considerations When Facing Reductions in Emergency Communications Budgets Fact Sheet

In addition, members developed and updated resources to assist stakeholders during times of constrained funding. Published in March, the *Contingency Planning Guide for Emergency Communications Funding (Contingency Planning Guide)* provides a comprehensive look at public safety officials’ considerations when planning for or facing budget reductions and recommends actions to take before, during, and after budget cuts. The Funding and Sustainment Committee also updated the *Contingency Considerations When Facing Reductions in Emergency Communications Budgets* fact sheet. The updated fact sheet provides a series of contingency considerations to justify investment in four mission-critical resource categories and refers readers to the more comprehensive *Contingency Planning Guide* for additional information.

TECHNOLOGY POLICY COMMITTEE

The Technology Policy Committee⁹ promotes the use of technologies, resources, and processes related to emergency communications and interoperability in coordination with NCSWIC. The Technology Policy Committee also encompasses the NG911 Working Group and the P25 User Needs Working Group (UNWG). In 2022, the Committee continued to support LMR systems, promote broadband technology and deployment, and encourage public safety information sharing. The Committee also worked with government partners to further the use and security of various technologies within the emergency communications ecosystem—Identity, Credential, and Access Management, NG911, advanced technologies, and cybersecurity.

⁸ Efforts undertaken by this Committee 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.

⁹ Efforts undertaken by the Committee directly contributed to NECP Objective 4.2; Success Indicator: Public safety organizations use up-to-date defined practices, procedures, pre-plans, specific venue/location response plans, incident type response plans, standard operating procedures, tactical response directives, and/or Tactical Interoperability Communications Plans that identify primary, secondary, and backup communications assets (e.g., networks, devices, and applications) for effective communications coordination and information sharing during planned events and incidents. Efforts also contribute to NECP Objective 5.1; Success Indicator: SAFECOM and NCSWIC identify public safety technology and infrastructure capability gaps.

Technology Policy Committee Accomplishments

Chair: Phil Mann

- ✓ [Communications Dependencies Case Study: Nashville 2020 Bombing](#)
- ✓ SAFECOM Nationwide Survey (SNS) Findings: Technology Trends and Recommendations to the Emergency Communications Preparedness Center (ECPC)
- ✓ IWCE Panel—Who Can and Should You Depend On?
- ✓ IAEM Panel—Be Prepared: Managing 3rd Party Dependencies in a Connected Ecosystem

The Technology Policy Committee released several products in 2022. The *Communications Dependencies Case Study: Nashville 2020 Bombing* document shares lessons learned and key takeaways from the Nashville, TN, bombing and provides public safety officials with knowledge to better prepare for severe communications outages and work with commercial providers and other partners to maintain and restore service. The Committee also developed the SAFECOM Nationwide Survey (SNS) Findings: Technology Trends and Recommendations to the Emergency Communications Preparedness Center (ECPC), which proposes potential opportunities for collaboration between SAFECOM, NCSWIC, and ECPC member departments to address public safety

technology trends and capability gaps. In 2022, Technology Policy members presented panel sessions at the International Wireless Communications Expo (IWCE) and the International Association of Emergency Managers (IAEM) Conference. The Committee also received a JamX 22 Operation Trinity presentation in March and participated in an on-site demonstration at the Orleans Parish Communications District and Real-Time Crime Center during the July in-person meeting in New Orleans, LA. Towards the end of 2022, the Committee drafted the *Paging: A Vital Link for Public Safety*, and the *LMR for Information Technology (IT) Professionals* documents, expected to be published in 2023.

P25 USER NEEDS WORKING GROUP: The P25 UNWG¹⁰ is a forum for education, discussion, and input on issues directly or indirectly related to the P25 Suite of Standards from a broad range of public safety users and subject matter experts. The UNWG has an informal advisory relationship with the P25 Steering Committee, subject to the approval and oversight of the Technology Policy Committee, SAFECOM, and NCSWIC. In 2022, the Working Group published a white paper on *LMR/Long Term Evolution (LTE) Interoperability: Best Practices*, as well as the *P25 UNWG Fact Sheet*. The P25 UNWG also developed a white paper on Link Layer Encryption (LLE) and Link Layer Authentication (LLA), explaining the difference between the two systems and why both are important. This paper is due for publication in 2023. The group also began planning for a Link Layer Security (LLS) Summit which will aim to create a common understanding among manufacturers of the user community’s challenges. Specifically, the summit will cover difficulties with the implementation and use of LLA’s features and functions; establish a collaborative and coordinated path forward to resolve identified issues with LLA; and identify appropriate actions that manufacturers will implement to ensure both effective operability and interoperability of upcoming LLE offerings and avoid continuing the present state of LLA offerings. The Global Positioning System (GPS) Focus Group completed five interviews with members of the public safety community on their GPS use to be compiled into a white paper for publication in 2023.

P25 UNWG Accomplishments

SAFECOM Co-Chair: Scott Wright

- ✓ [LMR/LTE Best Practices White Paper](#)
- ✓ [P25 UNWG Fact Sheet](#)
- ✓ Provided input to FPIC on recommendations for ISSI/CSSI standards modifications
- ✓ Five interviews conducted on the use of GPS

NG911 WORKING GROUP: The NG911 Working Group¹¹ utilizes stakeholder feedback from multiple levels of government and associations to identify short- and long-term priorities to support efforts to fund, assess readiness, and complete the transition to NG911. The NG911 Working Group helped Emergency Communications Centers (ECCs)/Public Safety Answering Points (PSAPs) to strengthen their cybersecurity posture through publications such as *Two Things Every 911 Center Should Do to Improve Cybersecurity* and the *Cyber Incident Response Case Studies*

¹⁰ Efforts undertaken by the Working Group directly contributed to NECP Objective 5.2; Success Indicator: SAFECOM and NCSWIC guide standards-based LMR evolution.

¹¹ Efforts undertaken by the Working Group directly contributed to NECP Objective 4.4; Success Indicator: ECCs/PSAPs address systems and staffing to support communications continuity-of-operations planning. Efforts also 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. Efforts also contribute to NECP Objective 6.2; Success Indicator: SAFECOM and NCSWIC encourage cybersecurity for NG911.

NG911 Working Group Accomplishments

Chair: Mark Buchholz

Vice Chair: Greg Holcomb

- ✓ *Cyber Incident Response Use Case Studies for ECC/PSAP Suite*
 - [Malware Attacks: Lessons Learned from an ECC](#)
 - [TDoS Attacks: Lessons Learned from a PSAP](#)
 - [Cyber Incident Response to PSAPs: A State's Perspective](#)
- ✓ *Considerations for Cyber Disruptions in an Evolving 911 Environment*
- ✓ [Two Things Every 911 Center Should Do to Improve Cybersecurity](#)
- ✓ *NG911 Incident-Related Imagery Impacts Webinar*
- ✓ [Manassas, VA GIS Use Case](#)
- ✓ *NENA Conference Sessions for Multimedia: Is Your Center Prepared and Cybersecurity for 911: What's New*
- ✓ *NG911 Interoperability Testing Model Webinar*
- ✓ *Preparing for Technological Transformation in ECCs*

for ECCs/PSAPs Suite. The *Case Studies* share lessons learned from states and localities responding to real-world cyberattacks, such as ransomware, Telephony Denial of Service (TDoS), and malware. The Working Group also developed the *Considerations for Cyber Disruptions in an Evolving 911 Environment* document to highlight considerations for ECCs when updating their Continuity of Operations (COOP) plans to better respond to cyber disruption events in a NG911 environment (anticipated publication March 2023). The Working Group engaged with the 911 community to raise awareness about the impacts of incident-related imagery and share best practices to help ECCs/PSAPs prepare for new technologies while also supporting the health and wellness of public safety telecommunicators. The *Preparing for Technological Transformation in ECCs* document highlights how ECCs can use emerging tools and technologies such as artificial intelligence (AI), remote dispatching, and integrated cloud technologies to supplement staffing, enhance data sharing, and improve delivery of critical emergency services (anticipated publication in 2023). The Working Group shared best practices for implementing essential location services through the *City of Manassas, Virginia Geographic Information System (GIS) Use Case*. The Working Group also partnered with

the DHS Science and Technology (S&T) Directorate to raise awareness about DHS S&T interoperability and conformance testing initiatives that are focused on strengthening the overall NG911 environment.

COMMUNICATIONS SECTION TASK FORCE

The Communications Section Task Force (CSTF)¹² addresses challenges associated with supporting ICT services within the National Incident Management System (NIMS) Incident Command System (ICS). The CSTF assisted CISA and the Federal Emergency Management Agency (FEMA) in developing the *ICT Functional Guidance*, which provides a framework to incorporate the full scope of services into the incident management organizational structure to meet the increasing demands for voice, data, and video capabilities. The CSTF identified 11 positions that will serve in the ICT Branch within NIMS ICS, to include:

- Auxiliary Communicator (AUXC)
- Communications Coordinator (COMC)
- Communications Unit Leader (COML)
- Communications Technician (COMT)
- Cybersecurity Planner (CYBP)
- Incident Communications Center Manager (INCM)
- Incident Tactical Dispatcher (INTD)
- Information Technology Service Unit Leader (ITSL)
- Information Technology Support Specialist (ITSS)
- Radio Operator (RADO)
- Unified Help Desk (HELP)

CSTF Accomplishments

Chair: Deputy Chief Chris Lombard

Vice Chair: Greg Hauser, North Carolina SWIC

- ✓ *ICT Functional Guidance*
- ✓ *COML Curriculum Updates*
- ✓ *ITSL position description, position task book, and training curriculum*

¹² Efforts undertaken by this Task Force directly contributed 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. Efforts also contribute to NECP Objective 3.3; Success Indicator: SAFECOM and NCSWIC develop training curriculums for additional positions within the Information Technology Service Unit. Efforts also contribute to NECP Objective 4.1; Success Indicator: Public safety organizations possess primary, secondary, and backup communications capabilities aligned with the NIMS ICS and share appropriate forms (e.g., ICS 205) illustrating the status of an agency's capabilities.

The CSTF continues to build out position descriptions, develop position task books and training course curricula for each ICT position in the functional guidance document.

ISFTF Accomplishments

Chair: Sheriff Paul Fitzgerald

- ✓ Conducted Operational PoCs, demonstrating the operational applicability of the ISF
- ✓ Coordinated with Iowa to apply the ISF principles to a CAD-to-CAD interoperability and NG911 assessment
- ✓ Managed and conducted an ISF Operational PoC at the Texas A&M Interoperability Institute
- ✓ Scoped a Technical PoC and submitted for R&D funding
- ✓ Developed a strategy to engage with the industry for design, development, and implementation of ISF Integration Layer function capabilities

INFORMATION SHARING FRAMEWORK TASK FORCE

The Information Sharing Framework Task Force (ISFTF)¹³ develops a data interoperability framework, including technical and operational standards to enable secure information flow between disparate public safety systems, and defines best practices for data/icon security and interoperability.

The ISFTF spent most of 2022 conducting Operational Proofs-of-Concepts (PoCs) and demonstrating the operational applicability of the Information Sharing Framework (ISF). During 2022, the ISFTF worked with the Iowa Department of Public Safety and multiple counties across Iowa to apply the ISF principles to a computer-aided dispatch (CAD)-to-CAD interoperability and NG911 assessment. In May, members of the ISFTF managed and conducted an ISF Operational PoC at the Texas A&M Interoperability Institute 2022 focused on situational awareness

leveraging video normalization, scaling, and sharing. The Operational PoC included taking video streams from various internet protocol cameras at the facility and drone footage and displaying the video content in an Esri GIS video sharing platform and blue force tracking application both on laptops and smartphones. In addition, the video content was presented on a web browser, Windows application, and Android mobile application via three clients. The next phase of the Operational PoC will incorporate Trustmarks, an emergency management platform, and a CAD system.

During 2022, the ISFTF also focused on scoping a Technical PoC, submitting for research and development (R&D) funding, and developing a strategy to engage with the industry for design, development, and implementation of ISF Integration Layer function capabilities. As a result, the ISFTF focus in 2023 will be engaging with platform providers, cloud providers, and companies currently involved in data exchange products and services in the public safety ecosystem.

P25 COMPLIANCE ASSESSMENT PROGRAM TASK FORCE

The P25 Compliance Assessment Program Task Force (CAPTF)¹⁴ provides public safety community input into the DHS S&T P25 CAP program, which assesses communications equipment compliance to the P25 Suite of Standards. In 2022, the P25 CAPTF provided the S&T P25 CAP program with user input and guidance on proposed Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) CAP interoperability testing, supported the temporary suspension of CAP ISSI/CSSI conformance testing, provided input into the proposed Multi-key Encryption Compliance Assessment Bulletin (CAB) update, and proposed CAP website content revisions.

P25 CAPTF Accomplishments

Chair: Chief Gerald Reardon

- ✓ Provided user input and guidance on proposed ISSI and CSSI CAP interoperability testing
- ✓ Supported temporary suspension of CAP ISSI/CSSI conformance testing
- ✓ Provided input into the proposed Multi-key Encryption CAB update
- ✓ Proposed CAP website content revisions

¹³ Efforts undertaken by the Task Force directly contributed to NECP Objective 5.3; Success Indicator: SAFECOM and 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.

¹⁴ Efforts undertaken by the Task Force directly contributed to NECP Objective 5.2; Success Indicator: SAFECOM and NCSWIC guide standards-based LMR evolution.

2022 MEETINGS

In-person meetings are an integral part of the SAFECOM program. CISA hosted a number of large and small in-person meetings throughout the year to promote collaboration and networking among members as well as determine solutions to some of the nation's most pressing issues on emergency communications interoperability. Below, please find select summaries for some of the group's larger in-person meetings. Full summaries of these in-person meetings may be found under the *Joint Meetings* or *SAFECOM Meetings* section of the [SAFECOM website](#).

In addition to the larger meetings, SAFECOM's sub-groups also met in-person and virtually throughout the year. Across 12 sub-groups, SAFECOM held 75 committee, working group, and task force meetings in 2022. Several sub-groups also presented at public safety and emergency communications conferences or state-level organizations.

SPRING 2022 BI-ANNUAL MEETING (JUNE 8-9; CORONADO, CA)

SAFECOM members convened in-person on June 8-9, in Coronado, California, beginning with a joint meeting with the NCSWIC and concluding with a stand-alone SAFECOM meeting. CISA Deputy Director Nitin Natarajan served as the keynote speaker, helping to kick off the event with opening remarks and CISA updates. Members of both programs heard sessions on building redundancy and resiliency in the face of third-party reliance, establishing standard talkgroup names for public safety broadband, transitioning to NG911, and understanding federal emergency communications funding opportunities. Members also received updates on the NIMS/ICT guidance document developed by the CSTF and FEMA and participated in a working session to update the *Public Safety Communications Evolution Brochure*. The following day, SAFECOM members reconvened and attended sessions on combatting unauthorized radio access, responding to the pandemic through the rapid establishment of systems in support of alternate care and testing sites, eliminating in-building wireless dead zones, and using unmanned aerial system and drone technology in public safety. Additionally, the group explored how the emergency communications community has changed during the pandemic, discussed key public safety issues on the horizon and ways SAFECOM can help solve these issues; received an update on CISA's priority services for emergency communications; and took in a SAFECOM membership spotlight on the All-Hazards Incident Management Teams Association (AHIMTA). View the [full summary](#) on SAFECOM's website.



Photo: SAFECOM Membership, December 2022

FALL 2022 BI-ANNUAL MEETING (DECEMBER 13-14; JACKSONVILLE, FL)

SAFECOM members came together for the second consecutive in-person meeting on December 13-14, in Jacksonville, Florida, where members received a keynote address from CISA Deputy Director Nitin Natarajan and heard real-world public safety communications successes and challenges in response to the Surfside building collapse and Hurricane Ian. SAFECOM also received updates on the CSTF's ICT Functional Guidance and from the Federal Communications Commission regarding public safety designated spectrum. Other sessions focused on CISA's new push for cyber resiliency in the 911 environment, protecting critical communications networks through LLA, and a SAFECOM membership spotlight on the Forestry Conservation Communications Association. In addition to the SAFECOM Meeting, members of several sub-groups met to further collaborate on identified work products, to include the SAFECOM Executive Board, SAFECOM Governance Committee, CSTF, and P25 UNWG. View the [full summary](#) on SAFECOM's website.

SAFECOM AT EXTERNAL CONFERENCES

SAFECOM members presented panel sessions at several significant public safety and emergency communications conferences in 2022, including the AHIMTA Education & Training Symposium, IWCE, National Emergency Number Association (NENA) 2022 Annual Conference & Expo, and IAEM Annual Conference. Sessions presented at these conferences are listed below:

- **National Sheriffs Association Meeting** (February 7; Washington, D.C.)
 - Demonstrated the operational applicability of the ISF, presented by members of the ISFTF
- **2022 AHIMTA Education & Training Symposium** (February 26-March 3; Denver, CO)
 - *Managing Information Technology (IT) for the IMT: A primer for the ITSL position* presented by members of the CSTF
- **IWCE 2022** (March 21-24; Las Vegas, NV)
 - *Cybersecurity and Infrastructure Security: Who Can and Should You Depend On?* presented by members of the Technology Policy Committee
 - *Are Your Radio Communications Really Secure? Why You Need Link Layer Authentication* presented by members of the P25 UNWG
- **NENA 2022 Annual Conference & Expo** (June 11-16; Louisville, KY)
 - *Cybersecurity for 911: What's New* presented by members of the NG911 Working Group
 - *Multimedia: Is Your Center Prepared* presented by members of the NG911 Working Group
- **IAEM Annual Conference** (November 11-17; Savannah, GA)
 - *Evolving the NIMS to Protect Information and Manage Communications Technology* presented by members of the CSTF
 - *Communications Used at Ad-Hoc and Temporary Vaccination and Hospital Sites* presented by members of the CSTF
 - *Be Prepared: Managing 3rd Party Dependencies in a Connected Ecosystem* presented by members of the Technology Policy Committee
- **Other**
 - National 911 Program State of 911 Webinar, *Impacts of Incident Related Imagery* presented by members of the NG911 Working Group (January 11)
 - Interoperability Institute at Texas A&M University, demonstrated the operational applicability of the ISF presented by members of the ISFTF (May 2022)
 - New York Area Science and Technology Forum on public safety interoperability in partnership with DHS S&T and the National Urban Security Technology Laboratory, demonstrated the operational applicability of the ISF presented by members of the ISFTF (August 2022)
 - Public Safety Communications Europe (PSCE) Winter Conference, demonstrated the operational applicability of the ISF presented by members of the ISFTF (December 6; Brussels, Belgium)

SAFECOM'S CONTRIBUTIONS TO NATIONWIDE GUIDANCE

SAFECOM members continued to support [National Emergency Communications Plan](#) implementation by completing activities aligned with each of the plan's goals and objectives. The 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 incorporates the plan's success indicators and implementation activities into its annual strategic planning and product development. With SAFECOM's contributions, significant progress has been made in the first three years of NECP implementation. Across the SAFECOM/NCSWIC workstream 52% (or 47 implementation activities) have been completed. Another 22% (or 20 implementation activities) are in-progress, resulting in nearly three quarters of planned activities either completed or started within three years.

SAFECOM members also contributed to the development of the latest iteration of the [SAFECOM Nationwide Survey \(SNS\)](#), which supplies essential data on emergency communications capability gaps that can be used to advocate for funding, establish priorities, and improve operations. The SNS measures progress made while identifying gaps in emergency communications and defining the range for new capabilities. SAFECOM members were directly involved in the review and update process for the upcoming SNS. Specific activities included individual participation on the question development working group (10 SAFECOM members, February-March 2022), review of the updated version of the survey by the entire membership (August 2022), and overall assistance in increasing awareness of the SNS among SAFECOM associations through brainstorming and direct marketing efforts. As the survey nears its launch date, SAFECOM members continue to serve as key conduits to the members of the emergency communications ecosystem and play a critical role in communicating the importance of the SNS data to potential respondents.

SAFECOM members also contributed to the [Fiscal Year 2022 SAFECOM Guidance on Emergency Communications Grants](#). Updated annually, this guidance offers current information on emergency communications policies, eligible costs, best practices, and technical standards for state, local, tribal, and territorial grant recipients investing federal funds in emergency communications projects.

LOOKING AHEAD TO 2023

Looking ahead to 2023, SAFECOM will continue to host regularly scheduled bi-annual SAFECOM meetings, as well as engage in public safety and emergency communications conferences. Members will present on several topics, such as:

- Evolving the NIMS to protect information and manage communications technology
- Public safety cybersecurity: new trends, insights, and resources
- Lessons learned for cyberattacks on 911
- Preparing for NG911: lessons learned from implementing GIS
- P25 technology and new P25 standards, interoperability, and security for 2023 and beyond
- Public-private collaboration in support of cutting-edge public safety research

SAFECOM aligns many of its priorities and initiatives to the nationwide goals established in the NECP. In 2023, SAFECOM will focus on enhancing public safety and emergency communications interoperability by:

- Publishing materials on statewide interoperability governance needs¹⁵
- Integrating emerging technology lessons learned and best practices into governance body resources and publicize new integration/adoption guidelines¹⁶
- Compiling legislative and regulatory issues associated with emerging technology¹⁷
- Showcasing available resources on emergency communications human factor principles¹⁸
- Identifying methods, practices, or procedures implemented to maintain highest degrees of readiness and information sharing about available communications capabilities¹⁹

¹⁵ Contributes to NECP Objective 1.1, Success Indicator: States and territories create or revise policy and plans to formalize and fund emergency communications governance bodies, such as Statewide Interoperability Governing Bodies.

¹⁶ Contributes to NECP Objective 1.3, Success Indicator: Governance bodies undertake technology integration and migration initiatives (e.g., broadband 911, alerts and warnings, information management, network infrastructure, cybersecurity) to guide implementation by public safety.

¹⁷ Contributes to NECP Objective 1.3, Success Indicator: Governance bodies identifying and addressing legislative and regulatory issues associated with emerging technology.

¹⁸ Contributes to NECP Objective 3.2, Success Indicators: Public safety organizations implementing mobile data applications utilize training and tools to ensure that responders effectively use and are not overloaded by available information. Public safety organizations implement tools and trainings to address emerging technology impacts.

¹⁹ Contributes to NECP Objective 4.1, Success Indicator: Public safety organizations possess primary, secondary, and backup communications capabilities aligned with the NIMS ICS and share appropriate forms (e.g., ICS 205) illustrating the status of an agency's capabilities.

- Identifying methods, practices, or procedures implemented on the use of personal devices for official public safety duties²⁰
- Identifying methods, practices, or procedures that most effectively implement and incorporate Priority Telecommunications Services (PTS), FirstNet, or other carrier offerings into existing public safety operations²¹

The 2023 SAFECOM Strategic Plan outlines a work plan for product development for the coming year. In addition to identifying key topics and activities to enhance public safety and emergency communications operability, interoperability, and security, SAFECOM took steps to ensure its strategic priorities align with the NECP. Some of SAFECOM’s guidance documents planned for publication in 2023 are:

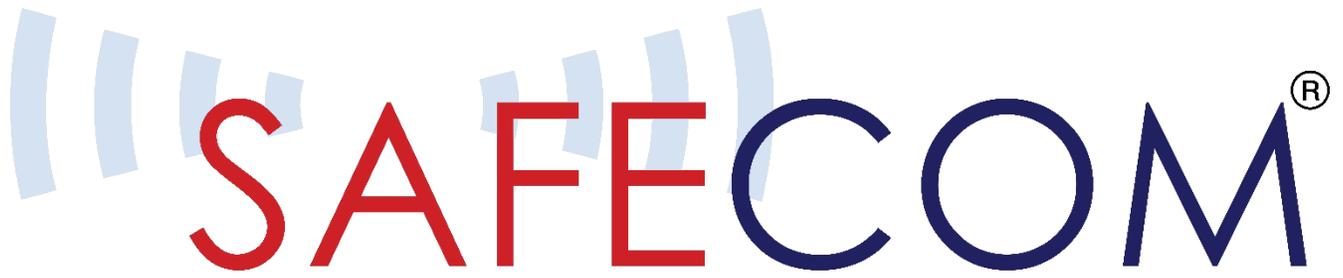
- | | |
|---|--|
| <ul style="list-style-type: none"> • <i>Writing Guide Standard Operating Guidelines (SOG)</i> • <i>SAFECOM Recommended Guidelines for Statewide Public Safety Communications Governance Structures</i> • <i>Guide to Getting Started with a Cyber Risk Assessment</i> • <i>“First 48:” What to Expect When a Cyber Incident Occurs</i> • <i>SAFECOM Cybersecurity Advisories</i> • <i>Public Safety Backup Best Practices</i> • <i>Public Safety Cloud Adoption Considerations</i> • <i>Cyber Risks to LMR: Second Edition</i> • <i>Public Safety Communications Evolution Brochure</i> • <i>FY23 SAFECOM Guidance on Emergency Communications Grants</i> • <i>Emergency Communications System Lifecycle Planning Suite</i> • <i>Grant Application Best Practices</i> • <i>Cybersecurity Funding and Emergency Communications: Advocating for Public Safety Priorities</i> • <i>Communications Dependencies Case Study: Hurricane Ian</i> | <ul style="list-style-type: none"> • <i>GPS: Configuring for LMR Systems and Mobile Devices</i> • <i>Governance of Machine Learning and AI in Public Safety</i> • <i>Preparing for Technological Transformation in ECCs</i> • <i>Considerations for Cyber Disruptions in an Evolving 911 Environment</i> • <i>Cybersecurity Solutions for the Evolving 911 Environment</i> • <i>Preparing for NG911 Guide</i> • <i>LLA and LLE: Are You Really Secure?</i> • <i>GPS for Public Safety: Use Cases and Best Practices</i> • <i>P25 in a Cloud-Based Environment</i> • <i>ICT Position Build Out</i> • <i>ICT Professional Development Path</i> • <i>ICT Incident Impact Measurements</i> • <i>Guidance in coordination with DHS S&T related to ISSI/CSSI conformance testing documents; interface testing; ongoing issues with emergency call cancel across interfaces; CAP testing related to LLA</i> • <i>ISF Technical Feasibility PoC</i> • <i>ISF Industry Request for Information</i> • <i>Initial ISF Deployment Strategy</i> |
|---|--|

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

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

²⁰ Contributes to NECP Objective 4.3, Success Indicator: Public safety organizations have recommended guidelines regarding the use of personal devices (e.g., bring your own device) based on applicable laws and regulations.

²¹ Contributes to NECP Objective 4.3, Success Indicator: Public safety organizations periodically review their use of PTS (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) and FirstNet, and ensure they have standard operating procedures governing the programs’ use, execution, and testing.



ASSURING A SAFER AMERICA THROUGH
EFFECTIVE PUBLIC SAFETY COMMUNICATIONS