ASSURING A SAFER AMERICA THROUGH EFFECTIVE PUBLIC SAFETY COMMUNICATIONS

SAFECOM Strategic Plan 2023

A guide to the program's short- and mid-term priorities

Publication: March 2023

SAFECOM®

CONTENTS

INTRODUCTION

The ***SAFECOM Strategic Plan*** describes the SAFECOM program's short- and mid-term priorities, and associated annual products and activities, to enhance operability, interoperability, and security for public safety communications through the education of the community, decision-makers, and elected officials. SAFECOM identifies these priorities annually through its committee structure, consisting of four standing committees: **Education and Outreach**, **Governance**, **Funding and Sustainment**, and **Technology Policy**. SAFECOM also utilizes working groups and task forces to accomplish initiatives. SAFECOM partners and coordinates closely with the National Council of Statewide Interoperability Coordinators (NCSWIC) across multiple program subgroups and engagements.

SAFECOM incorporates nationwide recommendations holistically, identifies gaps, and determines how to fill them. Drawing from the Cybersecurity and Infrastructure Security Agency's (CISA) major guiding documents, SAFECOM committees, working groups, and task forces develop strategic priorities to influence policy, guidance, and future efforts important to the public safety community. SAFECOM leveraged the following documents to develop its strategic priorities:

- *CISA 2023-2025 Strategic Plan*: Provides strategic direction on how the agency will collectively reduce risk and build resilience to cyber and physical threats to the nation's infrastructure
- *National Emergency Communications Plan* (NECP): Serves as the nation's strategic plan to enhance emergency communications capabilities
- *SAFECOM Nationwide Survey* (SNS): Nationwide data collection effort to obtain actionable and critical data that drives our nation's emergency communication policies, programs, and funding. SAFECOM leverages the collected data to identify gaps and inform the development of the program's strategic priorities and the Nationwide Communications Baseline Assessment
- *Nationwide Communications Baseline Assessment* (NCBA): Seeks to improve understanding across all levels of government on the capabilities needed and in use by today's emergency response providers to establish and sustain communications operability, interoperability, and continuity

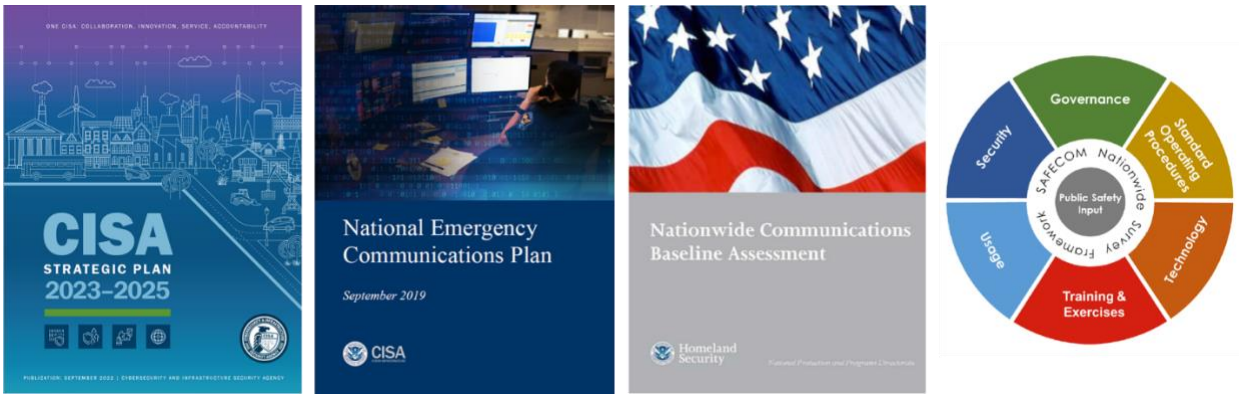

Figure 1: CISA's 2023-2025 Strategic Plan; NECP; NCBA; and SNS framework—major guidance documents developed by CISA and leveraged by the SAFECOM program to develop its strategic priorities.

The SAFECOM Executive Board, the program's leadership body, assumes the primary responsibility for maintaining and updating the *SAFECOM Strategic Plan* and will conduct annual revisions to ensure it is up-to-date and aligns with the changing internal and external interoperable emergency communications environment. In addition, the *SAFECOM Annual Summary* will track and report progress against the defined priorities and initiatives. This plan is a living document, which may be updated throughout the year as the emergency communications environment changes.

ABOUT SAFECOM

Established in 2001, SAFECOM is a stakeholder-supported public safety communications program administered by CISA. CISA supports SAFECOM's development of grant guidance, policy, tools, and templates, and provides direct assistance to state, local, tribal, territorial (SLTT), and federal practitioners. Through collaboration with emergency responders and policymakers across all levels of government, SAFECOM works to improve multi-jurisdictional and intergovernmental public safety communications interoperability. Working with the nation's leading public safety associations and SLTT government entities, SAFECOM guides the SLTT community in prioritizing public safety communications initiatives through its framework of strategic priorities and associated annual products and activities. This strategic direction helps SAFECOM execute its vision and mission.

OUR VISION

Assuring a safer America through effective public safety communications.

OUR 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.

SAFECOM ORGANIZATIONAL STRUCTURE

SAFECOM established a committee structure to better facilitate the way work products are developed.

Standing Committees are long-term, standing groups with a sustained focus on particular topics. The committees develop their own internal organization as they see fit, in coordination with CISA and SAFECOM leadership, to accomplish their work. This may include the formation of working groups within or across committees.

Working Groups exist for a pre-determined period of time as a subset of a committee.

Task Forces may be created to work for a short period of time, creating one defined product or executing one specific activity. Task forces are ad hoc and established at the direction of CISA and SAFECOM leadership.

SAFECOM and NCSWIC may operate joint efforts, including joint committees, working groups, and task forces.

SAFECOM adheres to a bottom-up approach, which means the program relies heavily on SLTT public safety communications stakeholders and policymakers for input and guidance as it works to define and implement interoperability solutions.

SAFECOM recognizes successful solutions must be based on the input of public safety communications stakeholders and policymakers across diverse disciplines, jurisdictions, and levels of government.

EDUCATION & OUTREACH

Promotes the role of SAFECOM and conveys SAFECOM's mission, goals, and priorities

GOVERNANCE

Improves governance structures & processes; Manages SAFECOM membership

FUNDING & SUSTAINMENT

Identifies innovative ways to fund and sustain systems and activities; Disseminates information on new funding sources

TECHNOLOGY POLICY

Promotes use of technologies, resources, and processes; Supports land mobile radio (LMR) systems; Promotes broadband technology & deployment; Encourages information sharing

2023 SAFECOM EXECUTIVE BOARD

The SAFECOM Executive Board provides strategic leadership and guidance to the SAFECOM Program.

SAFECOM CHAIR
Chief Gerald Reardon *(ret.)*
SAFECOM Chair
SAFECOM At-Large, *City of Cambridge Fire Department (MA)*

SAFECOM FIRST VICE CHAIR
Deputy Chief Chris Lombard
SAFECOM At-Large, *Seattle Fire Department (WA)*

SAFECOM SECOND VICE CHAIR
Chief Jay Kopstein *(ret.)*
SAFECOM At-Large, *Division of Homeland Security and Emergency Services Communications and Interoperability Working Group (NY)*

EDUCATION & OUTREACH COMMITTEE CHAIR
Michael Davis
SAFECOM At-Large, *Ulster County 9-1-1 Emergency Communications (NY)*

BOARD MEMBER
Chief Douglas M. Aiken *(ret.)*
National Public Safety Telecommunications Council

GOVERNANCE COMMITTEE CHAIR
Major George Perera
SAFECOM At-Large, *Miami-Dade Police Department (FL)*

BOARD MEMBER
Captain Anthony Catalanotto *(ret.)*
SAFECOM At-Large, *Division of Homeland Security and Emergency Services Communications and Interoperability Working Group (NY)*

FUNDING & SUSTAINMENT COMMITTEE CHAIR
Lloyd Mitchell
Forestry Conservation Communications Association

BOARD MEMBER
Sheriff Paul Fitzgerald
National Sheriffs' Association

TECHNOLOGY POLICY COMMITTEE CHAIR
Phil Mann
American Public Works Association

BOARD MEMBER
Charlie Sasser
National Association of State Technology Directors

SAFECOM PRIORITIES

SAFECOM discussed, developed, and vetted its priorities through the committees, working groups, and task forces at their end-of-year meetings in 2022. This approach consisted of revisiting proposed initiatives, brainstorming the priority and feasibility of related projects for the coming year, and developing work plans for product development. These work plans are outlined in this document, with subgroups operating jointly or in coordination with NCSWIC listed first, followed by the subgroups operated only by SAFECOM. In addition, SAFECOM closely coordinated in the implementation of the NECP, which addresses gaps within emergency communications, reflects new and emerging technological advancements, and provides guidance to drive the nation toward a common end-state for communications. SAFECOM has taken steps to ensure its strategic priorities align with the NECP, as identified in the key products tables in this section.

FUNDING AND SUSTAINMENT COMMITTEE

The Funding and Sustainment Committee identifies innovative ways to fund and sustain emergency communications systems and activities (e.g., training, personnel) pertinent to SLTT stakeholders in coordination with both SAFECOM and NCSWIC. The Committee also disseminates information on appropriations and new funding sources available to the public safety community at all levels of government. In 2023, the Funding and Sustainment Committee will create and update a series of products to highlight strategies for maintaining and securing funding for emergency communications projects. Through monthly meetings, the group will also disseminate information on best practices and new or existing funding sources.

STRATEGIC PRIORITY 1: Identify methods to fund and sustain emergency communications priorities, including statewide interoperability governance and support throughout the system lifecycle, and disseminate to decision-makers, elected officials, and the general public

STRATEGIC PRIORITY 2: Disseminate information on federal appropriations and new funding sources available to the public safety community at all levels of government

STRATEGIC PRIORITY 3: Understand changes to the emergency communications funding environment and create guidance to assist decision-makers with budget considerations

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Fiscal Year (FY) 2023 SAFECOM Guidance on Emergency Communications Grants Review	Provides current information on national policies, eligible costs, best practices, and technical standards for SLTT grant recipients investing federal funds in emergency communications projects	Q1	2	1.2.3
Emergency Communications System Lifecycle Planning Suite	Provides a high-level review of the considerations relevant to each step of the system lifecycle, including best practices, resources, and a lifecycle planning tool	Q1 – Q3	3	1.2.3
Grant Application Best Practices	Details best practices for SLTT grant applicants to incorporate for success in applying for emergency communications grants	Q2 – Q4	1	1.2.3
Cybersecurity Funding and Emergency Communications: Advocating for Public Safety Priorities	Provides tips on how to advocate that emergency communications and public safety should be recipients of cybersecurity funding	Q3 – Q4	3	1.1.1
Speaker Series	Facilitates information-sharing by inviting SLTT officials to present their funding best practices to the Committee	Q1 – Q4	2	1.2.3

TECHNOLOGY POLICY COMMITTEE

The Technology Policy Committee promotes the use of technologies, resources, and processes related to emergency communications and interoperability in coordination with SAFECOM and NCSWIC members. The Technology Policy Committee and its affiliated Next Generation 911 (NG911) Working Group (WG) and Project 25 (P25) User Needs Working Group (UNWG)—with Global Positioning System (GPS) Focus Group—continue 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 ecosystem—Identity, Credential, and Access Management (ICAM), NG911, advanced technologies, and cybersecurity.

The NG911 Working Group 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 P25 UNWG provides a forum for education, discussion, and input from a broad range of public safety users and subject matter experts on issues directly or indirectly related to the P25 Suite of Standards. The UNWG has an informal advisory relationship with the P25 Steering Committee, subject to the approval and oversight of the Technology Policy Committee and SAFECOM.

STRATEGIC PRIORITY 4: Gather and draft lessons learned, best practices, policies, and plans supporting the effective development, integration, migration, and adoption of new technologies and interoperability solutions

STRATEGIC PRIORITY 5: Collaborate across organizations to consolidate and disseminate strategies to manage risk and increase the resilience of public safety technologies, tools, and networks

STRATEGIC PRIORITY 6: Identify public safety technology and infrastructure capability gaps

STRATEGIC PRIORITY 7: Communicate emerging technology impacts to the public safety community

STRATEGIC PRIORITY 8: Guide standards-based LMR evolution

STRATEGIC PRIORITY 9: Coordinate with SAFECOM, NCSWIC, or joint SAFECOM-NCSWIC committees and working groups to identify and address legislative and regulatory issues associated with emerging technologies, capabilities, and risks

STRATEGIC PRIORITY 10: Identify, document, and develop work products that will facilitate the transition to NG911, utilizing stakeholder feedback from multiple levels of government and associations *(NG911 WG)*

STRATEGIC PRIORITY 11: Provide recommendations for implementing GPS capabilities in the public safety community *(P25 UNWG)*

STRATEGIC PRIORITY 12: Engage a broad user community to recommend user needs to the P25 Steering Committee, the Federal Partnership for Interoperable Communications (FPIC), or other appropriate body for further action *(P25 UNWG)*

STRATEGIC PRIORITY 13: Develop or review and provide input on P25 education and outreach materials to expand knowledge on P25 features, interfaces, and standards *(P25 UNWG)*

STRATEGIC PRIORITY 14: Formalize information sharing with the FPIC Encryption Focus Group and provide input on educational materials *(P25 UNWG)*

STRATEGIC PRIORITY 15: Coordinate with the FPIC on identified Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) needs to develop recommendations for standards modifications, new Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Compliance Assessment Program (CAP) testing needs, and/or educational material development *(P25 UNWG)*

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Communications Dependencies Case Study: Hurricane Ian	Summarizes impacts to public safety communications systems during Hurricane Ian in September 2022, and provides lessons learned and best practices to address communications infrastructure and alerts and warnings challenges	Q1	4 & 5	4.2.1
GPS: Configuring for LMR Systems and Mobile Devices	Explains the components of GPS in LMR systems and mobile devices, highlights the benefits and challenges, and discusses the interaction with existing features	Q2	4	4.2.1
Governance of Machine Learning and Artificial Intelligence in Public Safety	Highlights the governance and implementation of machine learning and artificial intelligence (AI) within the public safety community, and provides real-world examples of how organizations are using the technology today	Q3	7 & 9	1.3.2
Preparing for Technological Transformation in Emergency Communications Centers (ECCs) **[NG911 WG]**	Highlights how ECCs can use emerging tools and technologies, such as AI, remote dispatching, and integrated cloud technologies, to supplement staffing, enhance data sharing, and improve delivery of critical emergency services	Q1	10	5.2.1
Considerations for Cyber Disruptions in an Evolving 911 Environment **[NG911 WG]**	Highlights considerations for ECCs when updating their Continuity of Operations (COOP) plans to better respond to cyber disruption events in a NG911 environment; contains a helpful checklist for ECCs to consult when updating their plans	Q1	10	4.4.2
Cybersecurity Solutions for the Evolving 911 Environment **[NG911 WG]**	Discusses the 911 security landscape, how it will change when ECCs/public safety answering points (PSAPs) implement NG911, and potential technology solutions	Q2	10	6.2.2
Preparing for NG911 Guide **[NG911 WG]**	Provides ECC/PSAP administrators with high-level steps to take when transitioning to NG911 to help establish a framework and NG911 transition plan, and highlights success stories of ECCs/PSAPs implementing new technologies	Q3	10	2.1.1
Geographic Information System (GIS) Resource **[NG911 WG]**	Helps agencies navigate addressing challenges with NG911 while using industry and United States Postal Service (USPS) standards	Q4	10	5.2.1
Link Layer Authentication (LLA) and Link Layer Encryption (LLE): Are You Really Secure? **[P25 UNWG]**	Summarizes the difference between LLA and LLE; emphasizes the need for encryption in the P25 environment and provides a case study for why LLA is needed	Q1	13	N/A
GPS for Public Safety: Use Cases and Best Practices **[P25 UNWG]**	Provides a view into P25 GPS capabilities, its uses, and examples of how GPS is currently being used by public safety practitioners	Q1	11	N/A

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
***Link Layer Security (LLS) Summit* [P25 UNWG]**	Brings together users and manufacturers to discuss current LLA challenges, use case examples, and LLE standards development	Q3	13 & 15	N/A
***P25 in a Cloud-Based Environment* [P25 UNWG]**	Explains how to connect to a cloud-based solution, where the system is located, and highlights the physical, security, and operational risks of moving a LMR system to a cloud-based environment	Q4	13	5.2.2
***LLS Video* [P25 UNWG]**	Documents LLS benefits, challenges, and use cases in the public safety community through a short educational video	Q4	13	N/A

COMMUNICATIONS SECTION TASK FORCE

The Communications Section Task Force (CSTF) addresses challenges associated with supporting information and communications technology (ICT) within the National Incident Management System (NIMS) Incident Command System (ICS). In 2022, the CSTF, together with the Federal Emergency Management Agency (FEMA), developed a functional guidance document to outline the roles and responsibilities needed to enhance NIMS ICS in support of ICT functions. The CSTF's goal for 2023 is to support ICT implementation. The CSTF members are committed to reengage the ICT community through the following means:

- Use the ICT functional guidance as marketing tool
- Urge SAFECOM representatives to encourage their organizations to promote the ICT function
- Provide guidance and best practices for local utilization of ICT in ICS structures

A primary activity of the task force in 2023 is building out position descriptions, position task books, and course curricula for each ICT position in the functional guidance document.

STRATEGIC PRIORITY 16: Promote and provide consistent recruitment, training, retention, and support for ICT personnel

STRATEGIC PRIORITY 17: Support the development of national standards for qualification, certification, and credentialing for ICT personnel

STRATEGIC PRIORITY 18: Update the ICT course curriculum, as needed

STRATEGIC PRIORITY 19: Build out new ICT branch positions, including cyber unit positions and functions

STRATEGIC PRIORITY 20: Provide clarification of existing position descriptions to include the all-hazards environment

STRATEGIC PRIORITY 21: Engage the ICT community to identify active participants and share related updates

STRATEGIC PRIORITY 22: Streamline the instructor requirements for ICT Train-the-Trainer courses

STRATEGIC PRIORITY 23: Identify governance needs for the task force and the Incident Communications Advisory Committee (ICAC) to develop and support ICT implementation

STRATEGIC PRIORITY 24: Continue to promote the alignment of the ICT function beyond the branch level and influence its inclusion as a section within an ICS structure

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
ICT Position Build Out	Develops/updates position descriptions, position task books, and training courses of ICT positions; priorities include Communications Unit Leader (COML), Communications Technician (COMT), Information Technology Service Specialist (ITSS), Cyber Planner (CYBP), and Communications Coordinator (COMC)	Q1 – Q4	17, 18, 19, 20	3.1.3, 3.3.3
Professional Development Path	Documents a professional development path for communications staff to increase their ICT support capabilities	Q3	16	3.1.3, 3.3.3
Communications Unit Community	Explores online platforms for sharing ICT best practices and challenges and identifying implementation solutions	Q3	16, 21	3.1.3, 3.3.3
Incident Impact Measurements	Collects data on ICT implementation to analyze effectiveness of the functional guidance and propose further changes	Q2 – Q4	16	3.1.3, 3.3.3

PROJECT 25 COMPLIANCE ASSESSMENT PROGRAM TASK FORCE

In coordination with NCSWIC, the P25 Compliance Assessment Program Task Force (CAPTF) provides public safety community input into the DHS S&T P25 CAP, which assesses the compliance of communications equipment with the P25 Suite of Standards.

STRATEGIC PRIORITY 25: Continue coordination with DHS S&T on the development and implementation of ISSI/CSSI conformance and interoperability testing

STRATEGIC PRIORITY 26: Engage with the SAFECOM-NCSWIC P25 UNWG to develop interoperability and compliance testing requirements based on new/evolving user needs

STRATEGIC PRIORITY 27: Provide input and guidance to DHS S&T on future compliance testing priorities

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
ISSI/CSSI Conformance Testing Documents Input and Guidance	Reviews *ISSI/CSSI Conformance Test Tool Validation* document (December 2022) developed by DHS S&T	Q1	25	5.2.2
SAFECOM/NCSWIC P25 UNWG Engagement	Engages with the P25 UNWG as needed to share newly identified public safety user needs for standards recommendations	Ongoing	26	5.2.2
Interface Testing Input and Guidance	Provides guidance to DHS S&T CAP on Interworking Function (IWF) and Long-Term Evolution (LTE)/LMR interface testing once revised standards are published	Q3 – Q4	27	5.2.2
Ongoing Issues with Emergency Call Cancel Across Interfaces Guidance	Provides guidance to DHS S&T CAP on emergency call cancel compliance testing across interfaces	Q2 – Q4	27	5.2.2
CAP Testing Related to LLA Guidance	Provides recommendations on LLA compliance testing procedures and requirements as needed	Q3 – Q4	27	5.2.2

INFORMATION SHARING FRAMEWORK TASK FORCE

SAFECOM and NCSWIC established the Information Sharing Framework Task Force (ISFTF) to develop an Information Sharing Framework (ISF) to ensure the effectiveness of new products and technologies as agencies transition to mobile and fully interconnected environments. Making data interoperable and turning it into information that can be shared is a requirement that spans traditional boundaries. First responders should be able to discover, access, and consume relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, or location.

The *Approach for Developing an Interoperable ISF* document was published in November 2021 and Operational Proofs-of-Concepts (PoCs) were conducted in 2022 and will be completed in Q1 2023. During 2022, the ISFTF worked with the Iowa Department of Public Safety to apply the ISF principles to a computer-aided dispatch (CAD)-to-CAD interoperability and NG911 assessment. In addition, 2022 also focused on scoping a Technical Proof-of-Concept (TPoC), submission for research and development 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. Figure 2 below illustrates the ISFTF project stages.

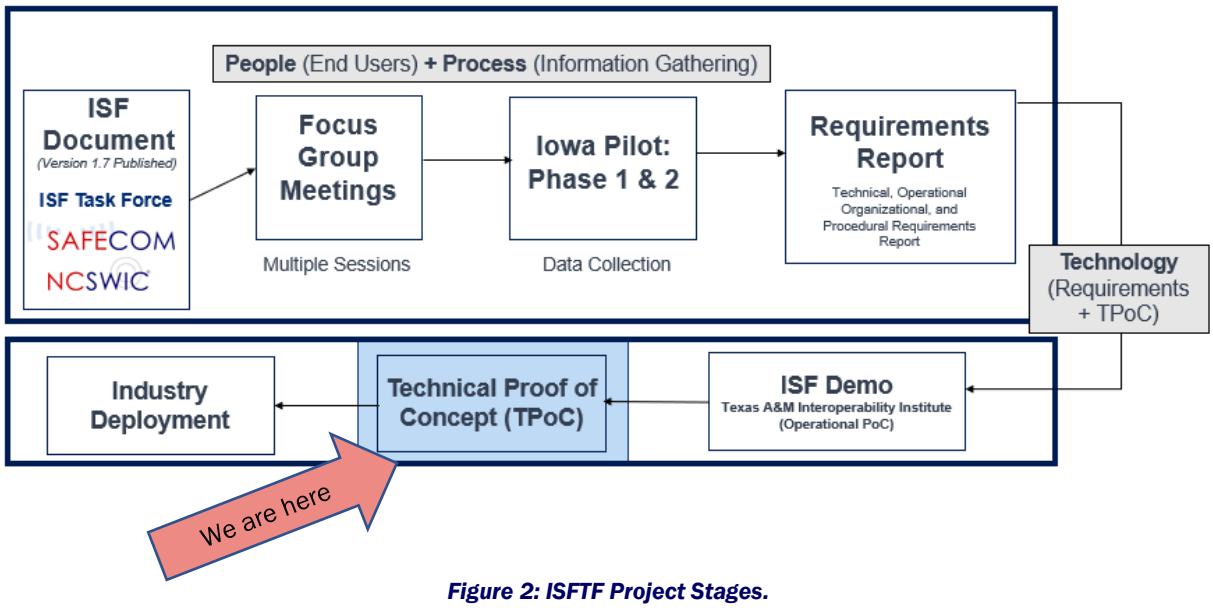

Figure 2: ISFTF Project Stages.

The TPoC will focus primarily on answering the three following questions regarding the ISF as a deployable product or product and service:

- Is the ISF platform technically feasible?
- Can the ISF be operationalized with measurable Key Performance Parameters (KPPs)?
- How will the ISF align with the public safety mission space for ease of use and increase in situational awareness?

In conjunction with the above questions, the ISFTF must also address the following development and deployment issues moving forward:

- Roles and coordination between 5G ecosystem players including telecommunications infrastructure service providers, cloud providers, and platform providers

- Excluding transport, determination of where integration layer functions reside in a hybrid wireless 4G/5G service provider and cloud provider architecture
- Determine ability to monitor and track KPPs end-to-end between emergency communications users on different provider networks
- Incorporation of emergency communications data formats
- ISF integration layer functions deployed as a holistic service with priority and security or partial service with customizable tools
- Role of AI in Analytics
- Incorporation of data privacy, regulatory, and jurisdictional considerations

STRATEGIC PRIORITY 28: Develop ISF TPoC to determine the technical feasibility of implementing information sharing common integration layer functions in a cloud computing environment and testing with public safety stakeholders

STRATEGIC PRIORITY 29: Begin developing a strategy for a "delivery mechanism" for ISF service and tools delivery to public safety and national security/emergency preparedness (NS/EP) stakeholders

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
ISF Technical Feasibility PoC	Determines technical feasibility of implementing information sharing common integration layer functions in a cloud computing environment and testing with public safety stakeholders	Q1 – Q4	28	5.3.3
ISF Industry Request for Information	Develops ISF platform by engaging or partnering with industry	Q1 – Q4	28	5.3.3
Initial ISF Deployment Strategy	Acts as a strategy for "delivery mechanism" for ISF service and tools delivery to public safety and NS/EP stakeholders	Q4	29	5.3.3

EDUCATION AND OUTREACH COMMITTEE

The Education and Outreach Committee promotes the role of SAFECOM and its impact on public safety communications nationwide. The Committee leads SAFECOM's communications efforts with member and non-member organizations to best convey SAFECOM's mission, goals, priorities, and success stories.

STRATEGIC PRIORITY 30: Bring awareness of SAFECOM's priorities, practices, and guidance to a broader group of stakeholders through engagements and SAFECOM publications

STRATEGIC PRIORITY 31: Create and update SAFECOM promotional materials (e.g., SAFECOM 101 presentation, promotional videos, elevator speech, podcast)

STRATEGIC PRIORITY 32: Assist all levels of government in identifying emergency communications gaps within the public safety community through the development and dissemination of education and outreach materials

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
***Public Safety Communications Evolution Brochure* Update**	Depicts the current public safety communications landscape, describes the evolution of public safety communications, and features considerations for how both LMR systems and LTE technology can operate concurrently during emergency response operations	Q1 – Q2	31	5.2.2

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Incident Communications Activity Report (ICAR) Marketing Materials	Promotes the release of the ICAR to the public safety community	Q1 – Q3	32	4.1.1
Association of Public-Safety Communication Officials (APCO) International Editorial Committee Engagement	Highlights SAFECOM's efforts in the public safety community in collaboration with the APCO Editorial Committee	Q1 – Q2	30	N/A
SAFECOM Outreach and Engagement Bi-Annual Report	Summarizes and analyzes the impacts of SAFECOM's 2023 outreach and engagement activities	Q2, Q4	30	N/A
SAFECOM National Public Safety Conference Booth Presence	Promotes a more robust SAFECOM booth presence at national/association public safety conferences to promote SAFECOM's mission, vision, and goals	Q1 – Q4	30	N/A
SAFECOM Membership Spotlight	Showcases the comprehensive experience of SAFECOM's membership and features how input from associations and at-large members drive improvements to the public safety community; Published as a blog post on the SAFECOM website	Q1 – Q4	31	N/A
SAFECOM Quarterly Newsletter	Promotes SAFECOM's most recent products and resources published by the SAFECOM membership on a quarterly basis	Q1 – Q4	32	N/A

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. The Governance Committee oversees the management of SAFECOM's membership and develops programmatic resources, such as SAFECOM's *Governance Charter*. Additionally, the Governance Committee maintains and administers the Marilyn J. Praisner SAFECOM Leadership Award, as well as the Cybersecurity Working Group. This working group shares actionable guidance and informational materials with peers regarding cybersecurity risks relevant to public safety communications. The Cybersecurity Working Group's objectives include sharing planning and mitigation guidance regarding known threats and vulnerabilities to public safety communications; consolidating and publishing information on cybersecurity services and grant programs; and working collaboratively with other groups to develop and share information on equipment and protocol vulnerabilities impacting the public safety mission.

STRATEGIC PRIORITY 33: Develop or revise nationwide guidance to elevate and formalize emerging communications technologies, issues, and needs that affect the public safety community

STRATEGIC PRIORITY 34: Assess the composition of representatives relevant to public safety communications and produce guidance on how to build adaptive strategies for updating governance membership reflective of the broader Emergency Communications Ecosystem

STRATEGIC PRIORITY 35: Use Emergency Communications Ecosystem composition assessments to identify SAFECOM's membership gaps and address them through active solicitation of new members annually

STRATEGIC PRIORITY 36: Manage internal programmatic documents and procedures (e.g., *SAFECOM Governance Charter*, SAFECOM Elections)

STRATEGIC PRIORITY 37: Identify and address legislative and regulatory issues associated with emerging communications technologies, issues, and needs that affect the public safety community

STRATEGIC PRIORITY 38: Support the development of cooperative cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., Memorandum of Understanding, Memorandum of Agreement, mutual-aid agreements)

STRATEGIC PRIORITY 39: Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
New Membership Process Maintenance	Assesses membership needs; collects and vets new applications for membership based on needs	Q1 – Q4	35	N/A
Annual SAFECOM Elections	Supports the electoral process to determine the leadership of the SAFECOM program	Q3 – Q4	36	N/A
***Writing Guide Standard Operating Guidelines (SOG)* Revision**	Assists communities in developing SOGs for public safety communications	Q1	33	1.1.2
***SAFECOM Recommended Guidelines for Statewide Public Safety Communications Governance Structures* Update**	Revises the 2018 *SAFECOM Recommended Guidelines for Statewide Public Safety Communications Governance Structures* to support the formalization and funding of governance bodies; Integrates lessons learned and best practices and publicize new integration/adoption guidelines	Q2	33	1.1.1; 1.3.1
Governance Promotional Campaign	Conducts promotional campaign to spread the importance of all governance issues and encourages the use of available tools and resources	Q2	33	1.1.2
***Guide to Getting Started with a Cyber Risk Assessment* [Cybersecurity Working Group]**	Assists public safety organizations in understanding the steps of a cyber risk assessment and how it can help strengthen operational and cyber resiliency	Q1	39	6.2.1
***"First 48:" What to Expect When a Cyber Incident Occurs* [Cybersecurity Working Group]**	Provides public safety administrators the immediate steps to take after a cyber incident. The playbook is inclusive of public safety and industry partner recommendations	Q1	39	6.2.1
***SAFECOM Cybersecurity Advisories* [Cybersecurity Working Group]**	Provides informational messaging on time-sensitive, critical cybersecurity alerts and notifications at the request of the working group leadership	Ongoing	39	6.2.1
***Public Safety Backup Best Practices* [Cybersecurity Working Group]**	Outlines public safety-specific best practices when deploying and managing data backups	Q1	39	6.2.1
***Public Safety Cloud Adoption Considerations* [Cybersecurity Working Group]**	Highlights public safety-specific considerations when adopting and managing cloud technology	Q2	39	6.2.1
***Cyber Risks to LMR: Second Edition* [Cybersecurity Working Group]**	Presents additional cybersecurity considerations and guidance for analog and digital LMR systems	Q3	39	6.2.1

IMPLEMENTATION

The SAFECOM Executive Board will review the *SAFECOM Strategic Plan* annually to gather input and garner buy-in from SAFECOM's leadership group. Based on recommendations from SAFECOM's various committees, working groups, and task forces, the SAFECOM Executive Board will formally adopt the *Strategic Plan* and use this document as a tool to help the Program prioritize resources, strengthen governance, address interoperability gaps, and educate and inform elected officials and stakeholders.

SAFECOM will use regularly scheduled Executive Board and bi-annual SAFECOM meetings to work closely with the committees, working groups, and task forces assigned to specific goals and initiatives. As a result, committee chairs will regularly report to the SAFECOM Executive Board on their identified goals and initiatives throughout the year to ensure success.

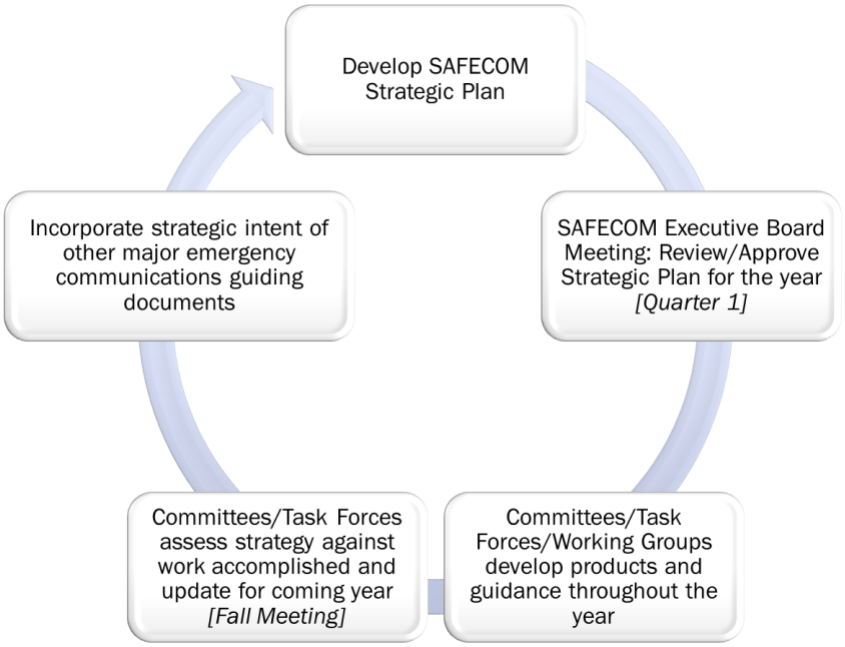

Figure 3: Strategy Implementation Cycle for the SAFECOM Strategic Plan.

For more information or to seek additional help, contact us at SAFECOMGovernance@cisa.dhs.gov.

ASSURING A SAFER AMERICA THROUGH EFFECTIVE PUBLIC SAFETY COMMUNICATIONS

SAFECOM® STRATEGIC PLAN 2023