SAFECOM®

2024 SAFECOM Strategic Plan

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

Publication: April 2024

CONTENTS

INTRODUCTION

The ***SAFECOM Strategic Plan*** describes the SAFECOM program's short- and mid-term priorities, and associated annual products and activities, with the intent of educating and providing recommendations for action to the public safety community, decision-makers, and elected officials to improve operability, interoperability, and security for emergency communications. SAFECOM identifies these priorities at the end of the calendar year through its standing committee structure: **Education and Outreach**, **Governance**, **Funding and Sustainment**, and **Technology Policy**. SAFECOM also utilizes its working groups and task forces[1] to identify and accomplish initiatives. Additionally, SAFECOM partners closely with the National Council of Statewide Interoperability Coordinators (NCSWIC) across multiple program subgroups and engagements to ensure a coordinated approach to identifying and executing emergency communications initiatives throughout the year.

SAFECOM incorporates nationwide recommendations holistically, identifies gaps, and determines how to fill them in their annual plan. Drawing from SAFECOM's and the Cybersecurity and Infrastructure Security Agency's (CISA) major guiding documents, strategic priorities within the SAFECOM Strategic Plan influence policy, guidance, and future efforts important to the public safety community on emergency communications.

SAFECOM aligns its Strategic Plan to the following documents:

- *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

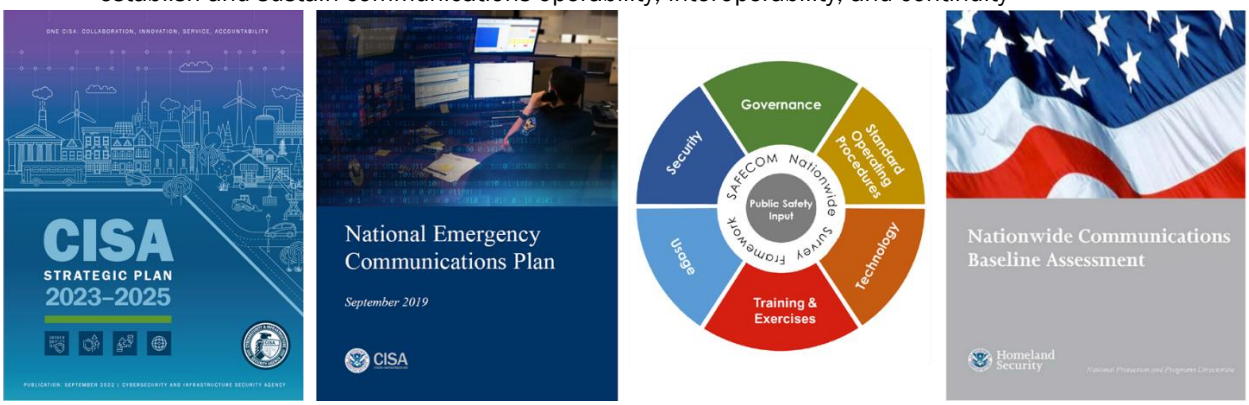

Figure 1: CISA's 2023-2025 Strategic Plan; NECP; SNS framework; and NCBA—major guidance documents developed by CISA and leveraged by the SAFECOM program to develop its strategic priorities.

The SAFECOM Executive Board, the program's leadership body, assumes primary responsibility for maintaining and updating the *SAFECOM Strategic Plan* and conducts annual revisions to ensure it is up-to-date and aligns with the changing needs of the emergency responder community. In addition, the *SAFECOM Annual Summary*

[1] While both groups are established for particular amounts of time, working groups are subsets of committees while task forces are independently established to complete priorities for particular time periods and with specific intentions

tracks and reports 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 local, state, territorial, federal, and tribal practitioners. Through collaboration with emergency responders and policymakers across the U.S. government and Tribal Nations, SAFECOM works to improve multi-jurisdictional and intergovernmental communications that support our nation's emergency response providers, including through its framework of strategic priorities and associated annual products and activities. This strategic direction ultimately helps SAFECOM execute its vision and mission and improves nationwide operability, interoperability, and resilience.

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 local, state, territorial, federal, and tribal 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

2024 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
Assistant Chief Chris Lombard
SAFECOM At-Large, *Seattle Fire Department (WA)*

SAFECOM SECOND VICE CHAIR
Chief Jay Kopstein *(ret.)*
SAFECOM At-Large, *New York State Division of Homeland Security & Emergency Services (NY)*

EDUCATION & OUTREACH COMMITTEE CHAIR
Battalion Chief Cody Worrell
SAFECOM At-Large, *Surprise Fire Department (AZ)*

FUNDING & SUSTAINMENT COMMITTEE CHAIR
Lloyd Mitchell
Forestry Conservation Communications Association

GOVERNANCE COMMITTEE CHAIR
Major George Perera
Major County Sheriffs of America

TECHNOLOGY POLICY COMMITTEE CHAIR
Phil Mann
American Public Works Association

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

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

BOARD MEMBER
Sheriff Paul Fitzgerald
National Sheriffs' 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 2023. 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. This document outlines the work plan in the following order: subgroups operating jointly with NCSWIC and then subgroups operated only by SAFECOM. SAFECOM has taken additional 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). The Committee also disseminates information on appropriations and new funding sources available to the public safety community at all levels of government. In 2024, 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 to Committee members.

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) 2024 SAFECOM Guidance on Emergency Communications Grants and Accompanying Materials 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 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	3	1.2.3
Grant Application Best Practices Hub	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
The Financial Benefits of Sharing Systems	Describes the financial benefits of sharing communications systems across jurisdictions via cost avoidance or cost reduction	Q4	1	1.2.3
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, SAFECOM, and NCSWIC.

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 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 Working Group [WG])

STRATEGIC PRIORITY 11: Engage a broad user community to identify emerging and shifting user needs and identify actions to address these needs (P25 UNWG)

STRATEGIC PRIORITY 12: Develop or provide input to P25 education and outreach materials to expand knowledge on P25 features, interfaces, and standards (P25 UNWG)

STRATEGIC PRIORITY 13: Coordinate with manufacturer and stakeholder groups on identified user needs to develop recommendations for existing P25 standards modifications, new P25 standards, new/revised Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Compliance Assessment Program (CAP) testing needs, and educational material development (P25 UNWG)

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Technology Policy Speaker Series	Provides information from experts related to cybersecurity, encryption, cloud policy, LMR/LTE integration, and funding & sustainment during quarterly sessions at Technology Policy Committee meetings	Q1-Q4	5	N/A
Public Safety Unmanned Aircraft System (UAS) Resource Guide	Provides information on UAS, their impacts on public safety operations, and how the public safety community can establish their own drone programs; Serves as an update to the 2021 *Public Safety UAS Resource Guide* developed by the Technology Policy Committee	Q1	5	N/A
Communications Dependencies Case Study: Maui Wildfires	Summarizes impacts to public safety communications systems during Maui Wildfires in August 2023, and provides lessons learned and best practices to address communications infrastructure and alerts and warnings challenges	Q2	4	N/A
Artificial Intelligence (AI) Webinar	Provides information regarding AI through a hosted webinar for SAFECOM and NCSWIC	Q3	9	N/A
911 Cybersecurity Resource Hub [NG911 Working Group]	Compiles cybersecurity resources by category through an interactive tool (e.g., website) for Emergency Communications Centers (ECC)	Q1	10	6.2.2
AI Integration in 911 Centers [NG911 Working Group]	Provides information regarding AI integration in 911 centers via a white paper or use case	Q2	10	5.2.1
Mitigate Swatting Threats Awareness Resource [NG911 Working Group]	Raises awareness about Secure Telephone Identity Revisited (STIR)/Signature-based Handling of Asserted Information Using toKENs (SHAKEN) technologies to mitigate swatting threats	Q3	10	6.2.2
Emergency Communications Cybersecurity Center (EC3) [NG911 Working Group]	Discusses the vision of Emergency Communications Cybersecurity Center (EC3) concept and how it will work	Q4	10	6.2.2
TBD Geographic Information System (GIS) Resource [NG911 Working Group]	Helps agencies navigate and address challenges with NG911 while using industry and United States Postal Service (USPS) standards and challenges with Computer-Aided Dispatch (CAD) systems being unable to read the Civic Location Data Exchange Format (CLDXF), which is used in the NENA i3 standard	Q4	10	5.2.1 5.2.5

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Global Positioning System (GPS) for Public Safety Location Services White Paper [P25 UNWG]	Examines P25 GPS through the lens of public safety practitioners tasked with providing real-time location capabilities to their agencies; explores real-world applications of P25 GPS, its limitations, and implementation considerations as learned through a series of interviews, a review of the P25 technical standards, and research into current application of GPS technology for public safety	Q1	12	5.2.2
Link Layer Authentication (LLA) Video [P25 UNWG]	Provides an overview of how LLA works to secure P25 LMR systems and provides real life examples of LLA systems in use	Q2	12	5.2.2
White Paper/Use Cases on the Need for Improved Frequency Capacity Efficiencies for Conventional P25 Networks [P25 UNWG]	Develops problem statement for non-traditional public safety entities' needs to access P25 systems for emergency preparedness, response, and recovery operations	Q3	11, 12, 13	5.2.2
Prioritized List of Link Layer Encryption (LLE) Standards for Development [P25 UNWG]	Provides the Telecommunications Industry Association (TIA) guidance on the P25 user community's priorities for the development of the LLE P25 Standards	Q2 & Q4	13	5.2.2
Process for Communicating P25 User Needs to TIA and P25 Steering Committee [P25 UNWG]	1) Establishes a repeatable, standardized process for interacting with TIA and the Steering Committee; 2) Conducts joint UNWG/TIA meeting; 3) Hosts Link Layer Security (LLS) Summit with TIA manufacturers	1) Q1 2) Q2 3) Q4	13	5.2.2
Address Paging and Alerting Needs [P25 UNWG]	Researches user communities (to include small, rural, and large city public safety agencies) current paging/alerting solutions; identifies best practices and lessons learned; identifies potential standards recommendations or educational material needs	Q4	11, 12, 13	5.2.2
UNWG Informational Video [P25 UNWG]	Educates user community on P25 standards development and recruits stakeholder participation in P25 UNWG	Q2	12	5.2.2
LMR In a Cloud-Based Environment [P25 UNWG]	Provides information on cloud-based solutions, highlighting the physical, security, and operational risks of moving an LMR system to a cloud-based environment	Q4	12	5.2.2
Address the Transition from LMR To LTE [P25 UNWG]	Identifies trends in public safety user base switching from P25 to other LTE-based technologies; discusses costs and increased or decreased coverage; may inform new P25 standards development and/or feature sets	Q4	11, 12, 13	5.2.2

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 14: Continue coordination with DHS S&T on the development and implementation of Inter-RF Subsystem Interface (ISSI)/Console Subsystem Interface (CSSI) conformance and interoperability testing

STRATEGIC PRIORITY 15: Engage with the SAFECOM-NCSWIC P25 UNWG and Federal Partnership of Interoperable Communications (FPIC) as needed to develop interoperability and compliance testing requirements based on new/evolving user needs

STRATEGIC PRIORITY 16: Provide input and guidance to DHS S&T on future compliance testing priorities

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Respond to DHS S&T requests on current and emerging topics	Reviews ISSI/CSSI conformance test tool validation documents developed by DHS S&T	Q1 – Q4	14	5.2.2
Engage with UNWG and FPIC	Engages with the P25 UNWG and FPIC as needed to share newly identified public safety user needs for P25 standards recommendations	Q1 – Q4	15	5.2.2
Guidance on Emergency Call Cancel Issues	Provides guidance as needed to DHS S&T CAP on ongoing issues with emergency call cancel compliance testing across interfaces	Q1 – Q4	16	5.2.2
Recommendations on LLA Compliance Testing Procedures and Requirements	Provides recommendations on LLA compliance testing procedures and requirements as needed to DHS S&T	Q1 – Q4	16	5.2.2
Monitor LLE P25 Standard Development	Monitors updates from UNWG on LLE P25 Standard development and provide guidance for CAP testing as needed	Q1 – Q4	15	5.2.2

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's (NIMS) Incident Command System (ICS). In 2022, the CSTF, together with CISA and the Federal Emergency Management Agency (FEMA), developed functional guidance to outline the roles and responsibilities needed to enhance NIMS ICS in support of ICT functions. The CSTF's goal for 2024 is to continue to support ICT implementation. The CSTF established four "action teams" to achieve each of the 2024 strategic priorities.

STRATEGIC PRIORITY 17: Update the ICT course curriculum

STRATEGIC PRIORITY 18: Support the development of national standards for qualification, certification, and credentialing for ICT personnel

STRATEGIC PRIORITY 19: Promote the alignment of the ICT function beyond the branch level and influence its inclusion as a section within an ICS structure

STRATEGIC PRIORITY 20: Establish and maintain a CSTF subgroup that supports the auxiliary communications (AUXCOM) function

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Update ICT Curriculum	Provides input on new or refreshed position descriptions (PD), priority position task books (PTB), and training courses for 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	3.1.3, 3.3.3
Recommend National Standards	Compiles database and best practices tool for states to set standards in qualification, certification, and credentialing of ICT personnel	Q1 – Q4	18	3.1.3, 3.3.3
Promote ICT	Markets and promotes the functional guidance and implementation best practices for audiences within and outside ICT	Q1 – Q4	19	3.1.3, 3.3.3
Establish and Sustain CSTF AUXCOM Subgroup	Promotes usage and inclusion of AUXCOM personnel within incident command and incident management organizational structures	Q1 – Q4	20	3.1.3, 3.3.3

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.

During 2022 to the present, the ISFTF has been supporting the Iowa Department of Public Safety to apply the ISF principles in defining requirements to acquire a computer-aided dispatch (CAD)-to-CAD interoperability capability. This process has been extremely valuable to the ISFTF as the team continues to optimize the ISF and customize it to real world use cases. Figure 2 below illustrates the ISFTF project stages and status as of Q1 2024.

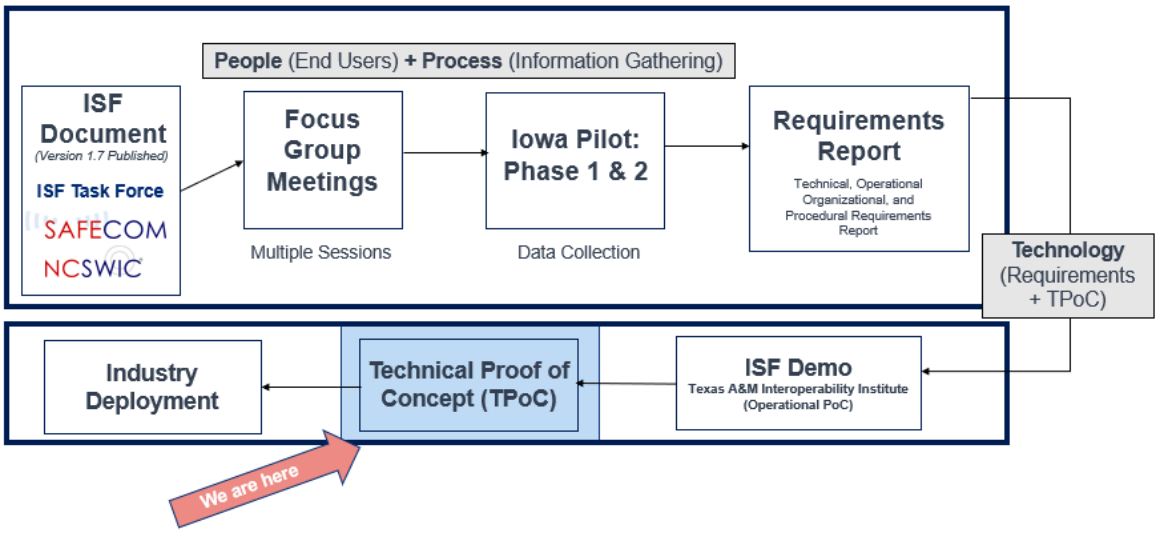

Figure 2: ISFTF Project Stages

A research and development (R&D) funding submission was written and approved for funding in 2023 resulting in the ISFTF working with DHS S&T to send out a Request for Information (RFI) to Industry in August 2023. The ISFTF reviewed the RFI submissions and held an ISFTF meeting in October 2023 to share results and discuss further engagement with Industry. Members of the ISFTF spent the rest of 2023 writing a detailed Statement of Objectives (SOO) for a Proof-of-Concept (PoC) to design, develop, test and implement the Integration Layer of the ISF as a service platform. The Technical PoC SOO will be released for proposals from Industry in early 2024 and must meet the four following objectives regarding the ISF as a deployable product or product and service:

- ISF Integration Layer capability must meet National Security and Emergency Preparedness (NS/EP) user base, including public safety and critical infrastructure personnel, mission requirements including functional, performance, and operational requirements
- Operationalize capability as a service platform and tools with ability to measure key performance parameters
- Industry adoption and ability to scale such a capability and deliver it to user base
- Ensure that this capability will provide greater situational awareness to public safety and other NS/EP users without overcomplicating or disturbing their mission

In conjunction with the above objectives, the Technical PoC and any deployment of the service platform must also address the following development and deployment issues moving forward:

- Roles and coordination between 5G and coming 6G 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 Key Performance Parameters 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 Integration Layer Function
- Incorporation of data privacy, regulatory, and jurisdictional considerations
- Incorporation of Federated ICAM and Trustmarks into Identity Management Integration Layer
- Analysis of impacts on ISF Integration Layer function in post quantum computing ecosystem, acceleration in complexity of AI, and future Intelligent Hyper-automation enhancements

STRATEGIC PRIORITY 21: Release detailed SOO for a PoC to design, develop, test and implement the Integration Layer of the ISF as a service platform to industry

STRATEGIC PRIORITY 22: Review SOO industry proposals and select performers for Technical PoC

STRATEGIC PRIORITY 23: Write and negotiate detailed Statement of Work (SoW) with selected performer(s)

STRATEGIC PRIORITY 24: Execute ISF Integration Layer as service platform Technical PoC as DHS S&T R&D project

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
ISF Service Platform SOO	Scopes SOO to design, develop, test, and implement the Integration Layer of the ISF as a service platform	Q1	21	5.3.3
SOO Proposal Review and Recommendations	Analyzes SOO proposals from industry and performer(s) selection	Q1-Q2	22	5.3.3

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
SoW for ISF Service Platform	Details scope of work to be done by performers with detailed schedule	Q2	23	5.3.3
Execute and Manage ISF Service Platform Technical PoC Project	Manages performer(s) as they design, develop, and test ISF service platform	Q4	24	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 25: Bring awareness of SAFECOM's priorities, practices, and guidance to a broader group of stakeholders through engagements and SAFECOM publications

STRATEGIC PRIORITY 26: Create and update SAFECOM promotional materials (e.g., SAFECOM Membership Spotlight, SAFECOM Factsheet, Introduction to SAFECOM Presentation, SAFECOM Quarterly Newsletter)

STRATEGIC PRIORITY 27: 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	Q3 – Q4	26	5.2.2
SAFECOM Product Promotion	Highlights SAFECOM's efforts in the public safety community in collaboration with the member association editorial efforts and SAFECOM Quarterly Newsletter	Q1 – Q4	25	5.3.3
SAFECOM Outreach and Engagement Bi-Annual Report	Summarizes and analyzes the impacts of SAFECOM's 2024 outreach and engagement activities	Q2, Q4	25	N/A
SAFECOM National Public Safety Conference Booth Presence	Promotes SAFECOM and its resources through staffing exhibit booths at national public safety conferences	Q1 – Q4	25	4.2.1
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; the Spotlight is published as a blog post on the SAFECOM web page	Q1 – Q4	26	N/A
SAFECOM Quarterly Newsletter	Promotes the most recent products and resources published by the SAFECOM membership on a quarterly basis	Q1 – Q4	25	5.3.3
SAFECOM Resource Library	Serves as a consolidated, alphabetized repository located on the CISA.gov/safecom website which showcases all of SAFECOM's resources and documents	Q1-Q2	34	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 28: Develop or revise nationwide guidance to elevate and formalize emerging communications technologies, issues, and needs that affect the public safety community

STRATEGIC PRIORITY 29: 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 30: Use Emergency Communications Ecosystem composition assessments to identify SAFECOM's membership gaps and address them through active solicitation of new members annually

STRATEGIC PRIORITY 31: Manage internal programmatic documents and procedures (e.g., *SAFECOM Governance Charter*, SAFECOM Elections)

STRATEGIC PRIORITY 32: Identify and address legislative and regulatory issues associated with emerging communications technologies, issues, and needs that affect the public safety community

STRATEGIC PRIORITY 33: 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 34: 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	30	N/A
Annual SAFECOM Elections	Supports the electoral process to determine the leadership of the SAFECOM program	Q3 – Q4	31	N/A
***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 publicizes new integration/adoption guidelines	Q1	28	1.1.1; 1.3.1

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Governance Promotional Campaign	Conducts promotional campaign to spread the importance of all governance issues and encourages the use of available tools and resources	Q2	28	1.1.2
Considerations for AI in Public Safety Communications	Emphasizes governance frameworks for implementation and usage of AI in public safety communications	Q1 – Q2	28, 32	1.1.2
Succession Planning for Public Safety Communications	Describes succession planning best practices both internal to SAFECOM and external for the public safety communications community	Q3	28, 30	1.1.2
Emerging Technology Webinars/Information Sharing Sessions	Provides live and/or recorded resources such as webinars on emerging technology (e.g., counter drones, jamming, NG911 implementation) of interest to the public safety communications community	Q1 – Q4	28, 32	1.1.2
Public Safety Cloud Adoption Considerations [Cybersecurity Working Group]	Highlights public safety-specific considerations when adopting and managing cloud technology	Q1	34	6.2.1
Data Backup Considerations for Public Safety [Cybersecurity Working Group]	Outlines public safety-specific best practices when deploying and managing data backups	Q1	34	6.2.1
AI Activity [Cybersecurity Working Group]	To be determined activity focused on AI (e.g., webinar, fact sheet, case study)	Q2	34	6.2.1
Cyber Risks to Land Mobile Radio (LMR): Second Edition [Cybersecurity Working Group]	Presents additional cybersecurity considerations and guidance for analog and digital LMR systems	Q3	34	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 or CISA leadership	Q1 – Q4	34	6.2.1
External Presentations & Panels/Forums [Cybersecurity Working Group]	Receives briefings and presentations from CISA partners on programs and resources relevant to the working group's needs and interests	Q1 – Q4	34	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.

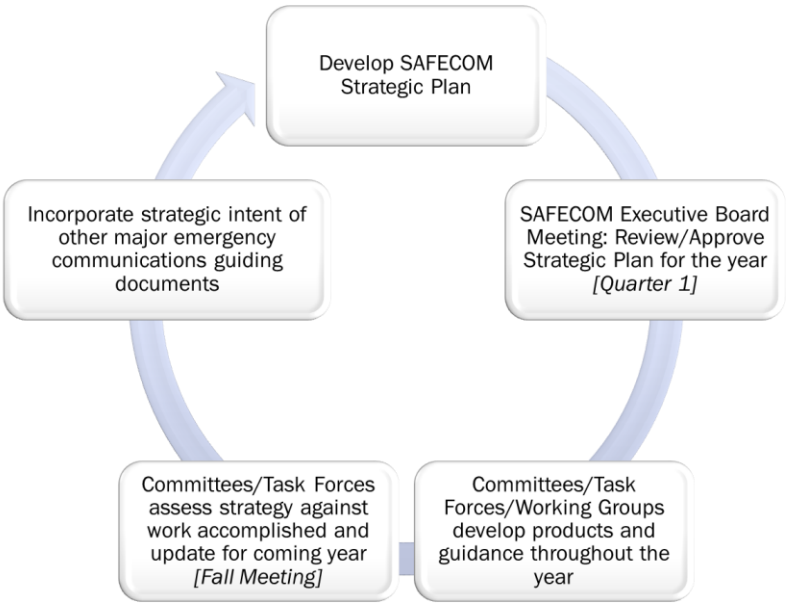

Figure 2: Strategy Implementation Cycle for the SAFECOM Strategic Plan.

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