SAFECOM®

ASSURING A SAFER AMERICA THROUGH EFFECTIVE PUBLIC SAFETY COMMUNICATIONS

2021 SAFECOM STRATEGIC PLAN

A guide to the Program’s short- and mid-term priorities

JUNE 2021

INTRODUCTION

The *SAFECOM Strategic Plan* describes the Program's short- and mid-term priorities, and associated annual products and activities, to enhance operability and interoperability 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:

- *National Emergency Communications Plan* (NECP): Serves as the Nation's strategic plan to enhance emergency communications capabilities
- *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 in order to establish and sustain communications operability, interoperability, and continuity
- *CISA Strategic Intent:* Lays out the strategic vision and operational priorities of the CISA Director, serving as a reference point to guide work and unify efforts across the organization

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. The Plan is a living document, which may be updated throughout the year as the emergency communications environment changes.

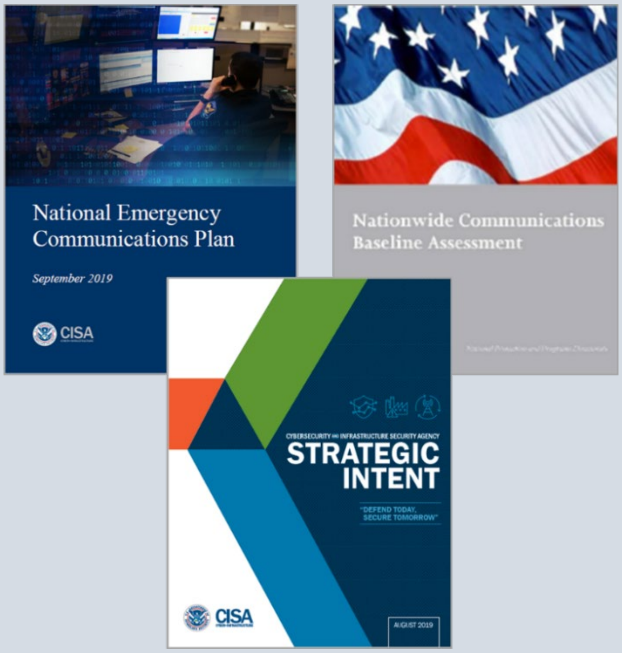

National Emergency Communications Plan
September 2019
CISA
Nationwide Communications Baseline Assessment
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
STRATEGIC INTENT
"DEFEND TODAY, SECURE TOMORROW"
CISA
AUGUST 2019

Figure 1: The National Emergency Communications Plan; Nationwide Communications Baseline Assessment, and CISA Strategic Intent—major guidance documents developed by CISA and leveraged by the SAFECOM Program to develop its strategic priorities.

CONTENTS

2021 SAFECOM EXECUTIVE BOARD

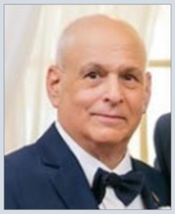
SAFECOM CHAIR

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

SAFECOM FIRST VICE CHAIR

Deputy Chief Chris Lombard
The InterAgency Board for Emergency Preparedness & Response
SAFECOM At-Large, *Seattle Fire Department (WA)*

SAFECOM SECOND VICE CHAIR



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

GOVERNANCE COMMITTEE CHAIR

Captain George Perera
SAFECOM At-Large,
Miami-Dade Police Department (FL)

EDUCATION & OUTREACH COMMITTEE CHAIR

Michael Davis
SAFECOM At-Large, *Ulster County 9-1-1 Emergency Communications (NY)*

FUNDING & SUSTAINMENT COMMITTEE CHAIR

Lloyd Mitchell
Forestry Conservation Communications Association

TECHNOLOGY POLICY COMMITTEE CHAIR

Phil Mann
American Public Works Association

BOARD MEMBERS

Chief Douglas M. Aiken
National Public Safety Telecommunications Council

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

Sheriff Paul Fitzgerald
National Sheriffs' Association

Charlie Sasser
National Association of State Technology Directors

WHO WE ARE

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 helped establish our vision and mission execution.

OUR VISION

Assuring a safer America through effective public safety communications

OUR MISSION

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

OUR COMMITTEES

EDUCATION & OUTREACH

PROMOTES role of SAFECOM
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

SAFECOM PRIORITIES

SAFECOM discussed, developed, and vetted its priorities through the committees, working groups, and task forces at their end-of-year meetings in 2020. This approach consisted of revisiting proposed initiatives, brainstorming the priority and feasibility of related projects for the coming year, and developing a work plan for product development. These work plans are laid out below, 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 *2019 NECP*, which addresses gaps within emergency communications, reflects new and emerging technological advancements, and provides guidance to drive the Nation towards a common end-state for communications. SAFECOM has taken steps to ensure its strategic priorities are in alignment 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 (i.e., training, personnel) pertinent to SLTT stakeholders in coordination with NCSWIC. The Committee also disseminates information on appropriations and new funding sources available to the public safety community at all levels of government.

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
Land Mobile Radio (LMR) Trio Document **Refresh**	Updates the LMR 101, LMR for Decision Makers, and LMR for Project Managers documents to align with the latest Project 25 and LMR standards, as well as the *SAFECOM Guidance on Emergency Communications Grants*	Q1	1	1.2.3
Fiscal Year 2021 SAFECOM Guidance on Emergency Communications Grants **Review**	Provides review and validation of the emergency communications priorities within the Guidance, as well as *Section 7. Funding Sources*	Q1	2	1.2.3
Legacy Document Refresh	Updates legacy Committee documents, available on the SAFECOM Funding Resources webpage, to align with new branding standards and available guidance	Q2 – Q3	1	1.2.3
System Lifecycle Planning Guide Template	Assists states in communicating needs and priorities to their elected officials	Q3	3	1.2.3
Contingency Planning Guide	Provides contingency considerations when facing reductions in emergency communications budgets and recommends priorities across three levels of funding	Q4	3	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 continues 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), Next Generation 911 (NG911), advanced technologies, and cybersecurity.

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: Through the Global Positioning System (GPS) Focus Group, provide a recommendation to comply with the Natural Resources Management Act *(Project 25 [P25] User Needs Working Group [UNWG])*

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

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

STRATEGIC PRIORITY 14: Document best practices and use cases for shared LMR systems, and LMR to Long-Term Evolution (LTE) systems *(P25 UNWG)*

STRATEGIC PRIORITY 15: Formalize information sharing with the FPIC Encryption Focus Group and provide input on educational materials *(P25 UNWG)*

STRATEGIC PRIORITY 16: Transition P25 User Needs Subcommittee (UNS) activities and responsibilities to the UNWG *(P25 UNWG)*

STRATEGIC PRIORITY 17: 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
Infrastructure Obstructions to Radio Propagation	Summarizes briefly passive and non-traditional sources of radio signal interference, including common practices to prevent or mitigate obstruction	Q1	5	N/A
Lessons Learned: Natural Disasters and Communications Dependencies	Identifies and summarizes lessons learned during various natural disasters and other emergencies in the previous few years	Q1 – Q3	4 & 5	4.2.2 4.2.3

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
GPS Working Group White Paper	Acts as the initial scoping paper to further define the GPS Focus Group and provide a recommendation for location services to comply with the Natural Resources Management Act	Q1	9 & 10	5.2.2
NG911 Geographic Information System (GIS) Use Cases	Highlights how states and localities are implementing GIS capabilities for NG911 (State of California and City of Manassas, Virginia are under development)	Q1 – Q4	10	5.2.1 5.2.5
Cybersecurity for 911 Centers	Raises awareness about cybersecurity for 911 centers and available federal and industry standards and recommendations to enhance the cybersecurity posture of NG911 systems	Q3	10	6.2.2
Federal Communications Commission Communications Security, Reliability and Interoperability Council's (CSRIC) VII Executive Summary	Provides an overview of the *CSRIC Security Risks and Best Practices for Mitigation in 911 Legacy, Transition and NG911 Implementations* report and highlights key recommendations and mitigation strategies	Q3	10	6.2.2
NG911 Disruption Guidance for 911 Centers	Provides guidance on disruption to calls and procedures at 911 centers	Q2	10	5.2.5 6.2.2
NG911 Data Management Fact Sheet	Provides guidance to 911 centers on managing data received from new technologies, such as connected buildings, smart cars, and panic buttons	Q4	10	5.2.1
Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) Repository	Serves as central location storing examples for agencies establishing or updating MOUs/MOAs for NG911	Q4	10	1.3.1 1.3.3 6.2.2
MOU/MOA Template	Provides example sections, descriptions, and contents of MOU/MOAs specifically addressing NG911 interoperability	Q2 2022	10	1.3.1 1.3.3 6.2.2
Engagement Plan with P25 Steering Committee and FPIC	Serves as the document guiding coordination between the P25 Steering Committee and FPIC to share information and provides broad user input on activities related to P25	Q2	12	N/A
P25 Education and Outreach Material Review	Provides suggestions to the P25 Steering Committee, FPIC, and P25 Technology Interest Group (PTIG) on P25 topics, and reviews and disseminates existing materials to a broad user community	Q4	12 & 13	5.2.2
LMR and LMR/LTE Best Practices	Provides best practices and lessons learned, including examples from users for LMR implementation, and LMR-to-LTE systems	Q3	14	5.2.2
Transition Activities from the P25 UNS to the UNWG	Formalizes transition of activities from the P25 UNS to the P25 UNWG	Q2	16	N/A
P25 CAP Test Cases	Supports coordination between the P25 CAP and SAFECOM CAP Task Force to develop CAP user test cases	Q3	17	N/A
Recommendations for Standards Modifications, New S&T CAP Testing Needs, and/or Educational Material Development	Leverages expertise from the FPIC ISSI Focus Group to develop ISSI/CSSI recommendations	Q3	17	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 (NIMS) Incident Command System (ICS). The CSTF continues to work towards developing a nationwide federated governance framework through the Incident Communications Advisory Council (ICAC), a focus group created to review and vet the CSTF's recommendations for enhancing the functionality of NIMS.

STRATEGIC PRIORITY 18: Promote and provide consistent recruitment, training, retention, and support for ICT personnel

STRATEGIC PRIORITY 19: Support the development of national standards for qualification, certification, and credentialing for ICT personnel

STRATEGIC PRIORITY 20: Update the ICT course curriculum, as needed

STRATEGIC PRIORITY 21: Establish new information technology (IT) positions and functions

STRATEGIC PRIORITY 22: Provide clarification of existing position descriptions (Communication Unit Leader [COML], Communication Technician, Radio Operator, etc.) to include the all-hazards environment

STRATEGIC PRIORITY 23: Engage the ICT community to identify active participants and share related updates

STRATEGIC PRIORITY 24: Streamline the instructor requirements for ICT Train-the-Trainer courses

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Incident Communications Metrics	Collects and synthesizes metrics to develop use cases to highlight how states and localities are unifying communications and IT functions under the same leadership	Q1 – Q3	19-21	3.3.2
ICAC Reengagement	Proposes reengaging with the ICAC to further collaborate on ICT	Q1 – Q2	23	N/A
***ICT Recruitment and Retention Plan* Implementation**	Proposes steps for implementing a plan to recruit, train, support, and retain candidates supporting information and communications management at planned events and incidents	Q1 – Q4	13-24	3.3.2
Federal Emergency Management Agency (FEMA) Supplemental Guidance	Draws from collaboration with FEMA to provide supplemental guidance supporting communications and information technology positions under NIMS ICS	Q3	19-21	4.1.1
COML Curriculum Updates	Reviews COML curriculum to ensure it is current	Q4	20	3.1.3
Position Description Updates	Leverages collaboration with FEMA National Integration Center (NIC) and the National Qualification System (NQS) to update communications and information technology positions (e.g., Radio Operator [RADO], Incident Communications Center Manager [INCM], Incident Tactical Dispatcher [INTD])	Q1 – Q3	20, 22	3.3.3
Emergency Support Function (ESF) #2 Lead Identification	Identifies a lead to oversee the qualification, training, certification, recognition, activation, and currency of ESF #2 and Communications Unit personnel	Q4	18	3.3.1
Communications Branch Modules	Develops modules for Communications Branch position-specific training and position descriptions	Q2	18, 20	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 P25 CAP, which assesses compliance of communications equipment to the P25 Suite of Standards.

STRATEGIC PRIORITY 25: Continue coordination with the 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 for new user needs requirements

STRATEGIC PRIORITY 27: Provide input and guidance to DHS S&T on the P25 Feature Gap project and future compliance testing priorities

STRATEGIC PRIORITY 28: Identify P25 CAP testing priorities that enhance overall communications security ("CommSec") via encryption and cybersecurity protections based on existing P25 standards

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
DHS S&T Coordination on Conformance and Interoperability Testing Priorities	Provides user input on the DHS S&T strategic planning for P25 conformance and interoperability testing priorities	Q4	27	5.2.2
SAFECOM-NCSWIC P25 UNWG Engagement	Supports coordination with the P25 UNWG on new interoperability and compliance testing requirements to share P25 interoperability challenges and successes	Q4	27	5.2.2

INFORMATION SHARING FRAMEWORK TASK FORCE

SAFECOM and NCSWIC established the Information Sharing Framework Task Force (ISFTF) comprised of IT and public safety communications interoperability subject matter experts from public safety agencies across the country. The ISFTF will develop an Information Sharing Framework (ISF) to ensure effectiveness of new products and technologies as agencies transition to mobile and fully interconnected environments. Making data interoperable and into information that can be shared is a requirement that spans beyond traditional boundaries. In addition, first responders should be able to discover, access, and consume any relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, and location.

The intended audience for the ISF is Statewide Interoperability Coordinators (SWICs) and other state-level communications personnel working in LMR, Broadband, 911, and state public alerts, warnings, & notifications systems all in alignment or directly involved in acquisition, management, and oversight of public safety emergency communications. The overarching goal of the ISF is to support transition to a common information exchange approach that a public safety community can adopt and use efficiently to make its emergency communications ecosystem interoperable.

STRATEGIC PRIORITY 29: Provide a customizable interoperability operational framework to identify and ensure alignment of people, processes, and technology prior to a major multi-agency, multi-jurisdiction event, that will:

- Inform a roadmap of actions taken by a public safety organization to have the most optimal impact on solving interoperability issues/gaps via governance, acquisition guidance, and alignment with training, exercises, and grants
- Inform and provide a checklist and guidebook for emergency communications acquisition decisions for products and services ensuring such acquisitions are interoperable, secure, resilient, and allow for data management
- Inform state leadership of the complexity and need for emergency communications interoperability across multiple networks/functions (e.g., LMR, Broadband, NG911, Computer-Aided Dispatch [CAD]/Records Management System [RMS], alerts/warnings, etc.)

- Aggregate all information sharing best practices, guidance, and lessons learned into one operational framework

STRATEGIC PRIORITY 30: Expand intended audience to include public safety IT personnel such as IT Service Unit Leaders (ITSL) and communications personnel such as the COML providing a common playbook on which to base future implementation decisions

STRATEGIC PRIORITY 31: Develop strategy to pilot a customization of the ISF for a use case in a simulated but real-world environment (e.g., outdoor lab), in alignment with a standards-based ICAM solution

STRATEGIC PRIORITY 32: Work with the Interoperable Communications Technical Assistance Program (ICTAP) to develop Technical Assistance (TA) offerings based on customization of ISF

STRATEGIC PRIORITY 33: Develop and publish white paper exemplar on ISF customization for video content sharing

STRATEGIC PRIORITY 34: ISF Proof-of-Concept (PoC) to determine technical feasibility of implementing information sharing common integration layer functions in a cloud computing environment and testing with public safety stakeholders

STRATEGIC PRIORITY 35: Begin developing strategy for "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 Final	Collects input from members regarding ISF structure for review by SAFECOM and NCSWIC in preparation for final release	Q1	29	5.3.3
ISF Customization Pilot Statement of Work and Test Plan	Develops strategy to pilot a customization of the ISF for a use case in a simulated but real-world environment (e.g., outdoor lab); includes alignment with a standards-based ICAM solution	Q3 – Q4	31	5.3.3
ISF Industry Request for Information	Develops ISF platform by engaging or partnering with industry	Q3 – Q4	34	5.3.3
Pilot/Table-Top for ISF Customization	Develops strategy to pilot a customization of the ISF for a use case in a simulated but real-world environment (e.g., outdoor lab). Current plan to execute in Q3 CY2021 at Interoperability Lab at Texas A&M University pending COVID-19 limitations	Q3 – Q4	31	5.3.3
ICTAP TA Course Content for ISF Customization	Provides content for TA offerings, in coordination with ICTAP, on customization of ISF to help public safety apply ISF to their specific jurisdiction, use case, inter-organization data exchange, and information sharing	Q3 – Q4	32	5.3.3
ISF White Paper Customization	Provides exemplar on ISF customization for video content sharing	Q1	33	5.3.3
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	Q3	34	5.3.3
Initial ISF Deployment Strategy	Acts as strategy for "delivery mechanism" for ISF service and tools delivery to public safety and NS/EP stakeholders	Q4	35	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, and priorities.

STRATEGIC PRIORITY 36: Bring awareness of SAFECOM's priorities, practices, and guidance to a broader group of stakeholders through engagements and SAFECOM publications

STRATEGIC PRIORITY 37: Create and update SAFECOM promotional materials (e.g., SAFECOM 101 presentation, promotional videos, elevator speech, podcast)

STRATEGIC PRIORITY 38: 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

STRATEGIC PRIORITY 39: Finalize and implement an effective digital media strategy

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
SAFECOM Website Maintenance	Supports ongoing website information updates	Q1 – Q4	36	3.2.1 3.2.2
SAFECOM-NCSWIC Quarterly Newsletter and Blogs	Provides information on new members, CISA updates, and articles from members on public safety interoperability	Q1 – Q4	36	1.1.1
***SAFECOM: Created by Public Safety Stakeholders to Strengthen Emergency Communications* Video**	Provides an overview of the importance of public safety interoperability, to be utilized at conferences and posted on the SAFECOM website	Q1	37	1.1.1
SAFECOM Outreach and Engagement Bi-Annual Report	Summarizes and analyzes the impacts of SAFECOM's outreach and engagement activities from January to June 2021	Q4	37	1.1.1
***Public Safety Communications Evolution Brochure* Update**	Updates the Public Safety Communications Evolution Brochure to reflect changes in the structure of CISA and the latest update to the SAFECOM Interoperability Continuum	Q4	37	5.2.2
SAFECOM Interoperability Continuum	Provides updates to the SAFECOM Interoperability Continuum to reflect changes to the emergency communications ecosystem	Q1	38	6.3.2
Incident Communications Activity Report (ICAR) Beta Testing	Supports coordination with the Communications Section Task Force in testing the Draft ICAR form with SAFECOM associations and at-large members to capture the emergency communications activity of any organized incident management command and coordination structure established for an Incident, Planned Event, or Exercise	Q1	38	4.1.1
SAFECOM Podcast Pilot	Supports development of SAFECOM Education and Outreach Committee digital outreach capabilities	Q4	39	1.1.1
SAFECOM Social Networking/Media Presence	Explores SAFECOM social media profiles to assist in outreach and engagement efforts and identifies other platforms for SAFECOM member communications	Q2	39	1.1.1

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

STRATEGIC PRIORITY 41: 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 42: Use Emergency Communications Ecosystem composition assessments to identify SAFECOM's membership gaps and address through active solicitation of new members annually

STRATEGIC PRIORITY 43: Identify and address legislative and regulatory issues associated with emerging communications technologies, issues, and needs that affect the public safety community

STRATEGIC PRIORITY 44: Support the development of cooperative cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., MOU, MOA, mutual aid agreements)

STRATEGIC PRIORITY 45: Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

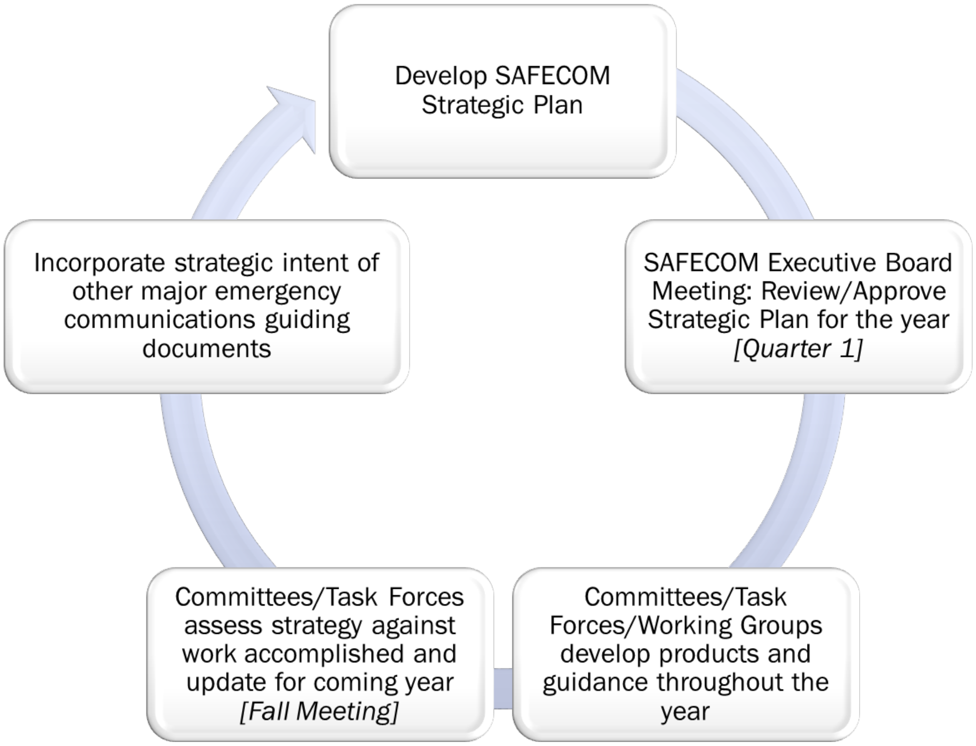
Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
***2018 SAFECOM Recommended Guidelines for Statewide Public Safety Communications Governance Structures* Update**	Supports the formalization and funding of governance bodies, integrates lessons learned and best practices for technology integration and migration initiatives, and publicizes new integration/ adoption guidelines	Q2	40	1.1.1 1.3.1
***Writing Guide for Standard Operating Procedures (SOP)/ Standard Operating Guidelines (SOG)* Revision**	Assists communities in developing SOPs/SOGs for public safety communications	Q2	40	N/A
Best Practices for Governance Charters Factsheet	Leverages suggested elements of governance charters and by-laws in the *Emergency Communications Governance Guide for SLTT Officials* (Governance Guide) to develop best practices for governance charters	Q2	40	1.1.2
Best Practices for Membership Analysis Factsheet	Articulates best practices in performing membership gap analyses in alignment with the evolving ecosystem and related partners	Q3	41	1.2.1
New Membership Process Maintenance	Assesses membership needs; collects and vets new applications for membership based on needs	Q1 – Q4	42	N/A

Product Name	Description	Timeline	Strategic Priority	NECP Success Indicator
Cybersecurity Guidance Factsheet ***[Cybersecurity Working Group]***	Advertises United States Computer Emergency Readiness Team (US-CERT) and other Information Sharing Environment (ISE) alerts and capabilities to the public safety community, including planning and mitigation guidance regarding known threats and vulnerabilities (e.g., Cyber Risks to NG911, Communications Resiliency Toolkit)	Q2	45	6.2.1
Cyber Resources Tracker ***[Cybersecurity Working Group]***	Provides awareness of cyber alerts, distributions, and subscriptions to inform stakeholders and lessen redundancy across channels, in coordination with the Governance Committee, Cybersecurity Working Group, and CISA	Q1 – Q2	45	6.2.1
Cyber Risks to LMR Whitepaper ***[Cybersecurity Working Group]***	Provides LMR background, examples of potential cyberattacks, and actionable steps to secure the system. Additional resources on planning and mitigation regarding known threats and vulnerabilities will also be included	Q1	45	6.2.1
The First 48 - Cyber Incident Response Best Practices Guide ***[Cybersecurity Working Group]***	Provides public safety administrators the immediate steps to take after a cyber incident. Intended to act as a playbook inclusive of public safety and industry partner recommendations	Q2	45	6.2.1
Cyber Incident Response Templates ***[Cybersecurity Working Group]***	Provides cybersecurity planning and cybersecurity incident response that encourage stakeholder customization	Q1 – Q2	45	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	45	6.2.1

IMPLEMENTATION

The SAFECOM Executive Board will review the *SAFECOM Strategic Plan* on an annual basis to gather input and garner buy-in from SAFECOM's leadership group. Based on recommendations from SAFECOM's various committees, task forces, and working groups, 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, task forces, and working groups 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.



Develop SAFECOM Strategic Plan

SAFECOM Executive Board Meeting: Review/Approve Strategic Plan for the year *[Quarter 1]*

Committees/Task Forces/Working Groups develop products and guidance throughout the year

Committees/Task Forces assess strategy against work accomplished and update for coming year *[Fall Meeting]*

Incorporate strategic intent of other major emergency communications guiding documents

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

SAFECOM®

ASSURING A SAFER AMERICA THROUGH
EFFECTIVE PUBLIC SAFETY COMMUNICATIONS