

MISSOURI STATEWIDE COMMUNICATION INTEROPERABILITY PLAN



April 2025

Developed by the Statewide Interoperability Executive Committee with support from the Cybersecurity and Infrastructure Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from the Statewide Interoperability Coordinator	1
Introduction.....	2
Interoperability and Emergency Communications Overview.....	3
Vision and Mission.....	4
Governance	4
Technology and Cybersecurity.....	7
Land Mobile Radio	7
911	8
Broadband.....	10
Alerts and Warnings.....	10
Cybersecurity.....	11
Funding.....	13
Implementation Plan	15
Appendix A: State Markers	18
Appendix B: Acronyms	28

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

Greetings,

As the Statewide Interoperability Coordinator (SWIC) for Missouri, I am pleased to present to you the 2025 Missouri Statewide Communication Interoperability Plan (SCIP). The SCIP represents the state's continued commitment to improving emergency communications interoperability and supporting public safety practitioners throughout the state. In addition, this update meets the requirement of the current U.S. Department of Homeland Security (DHS) grant guidelines.

Representatives from throughout the state collaborated to update the SCIP with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on governance, technology and cybersecurity, and funding. They are designed to support our state in planning for emerging technologies and navigating the ever-changing emergency communications landscape. They also incorporate the SAFECOM/National Council of SWICs (NCSWIC) State Interoperability Markers, which describe Missouri's level of interoperability maturity by measuring progress against 30 markers.

As we continue to enhance interoperability, we must remain dedicated to improving our ability to communicate among disciplines and across jurisdictional boundaries. With help from public safety practitioners statewide, we will work to achieve the goals set forth in the SCIP and become a nationwide model for statewide interoperability.

Sincerely,



Roger Strope
Missouri Statewide Interoperability Coordinator
Missouri Department of Public Safety

INTRODUCTION



The SCIP is a one- to three-year strategic planning document that contains the following components:

- **Introduction** – Provides the context necessary to understand what the SCIP is and how it was developed. It also provides an overview of the current emergency communications ecosystem;
- **Vision and Mission** – Articulates Missouri’s vision and mission for improving emergency and public safety communications interoperability over the next one- to three years;
- **Governance** – Describes the current governance mechanisms for communications interoperability within Missouri as well as successes, challenges, and priorities for improving it. The SCIP is a guiding document and does not create any authority or direction over any state or local systems or agencies;
- **Technology and Cybersecurity** – Outlines public safety technology and operations needed to maintain and enhance interoperability across the emergency communications ecosystem;
- **Funding** – Describes the funding sources and allocations that support interoperable communications capabilities within Missouri, along with methods and strategies for funding sustainment and enhancement to meet long-term goals;
- **Implementation Plan** – Describes Missouri’s plan to implement, maintain, and update the SCIP to enable continued evolution of, and progress toward, the state’s interoperability goals.

The Emergency Communications Ecosystem consists of many interrelated components and functions, including communications for incident response operations, notifications, alerts and warnings, requests for assistance and reporting, and public information exchange. The primary functions are depicted in the 2019 National Emergency Communications Plan.¹

¹ [2019 National Emergency Communications Plan](#)

The Interoperability Continuum, developed by the U.S. Department of Homeland Security's SAFECOM program and shown in Figure 1, serves as a framework to address challenges and continue improving operable/interoperable and public safety communications.² It is designed to assist public safety agencies and policy makers with planning and implementing interoperability solutions for communications across technologies.

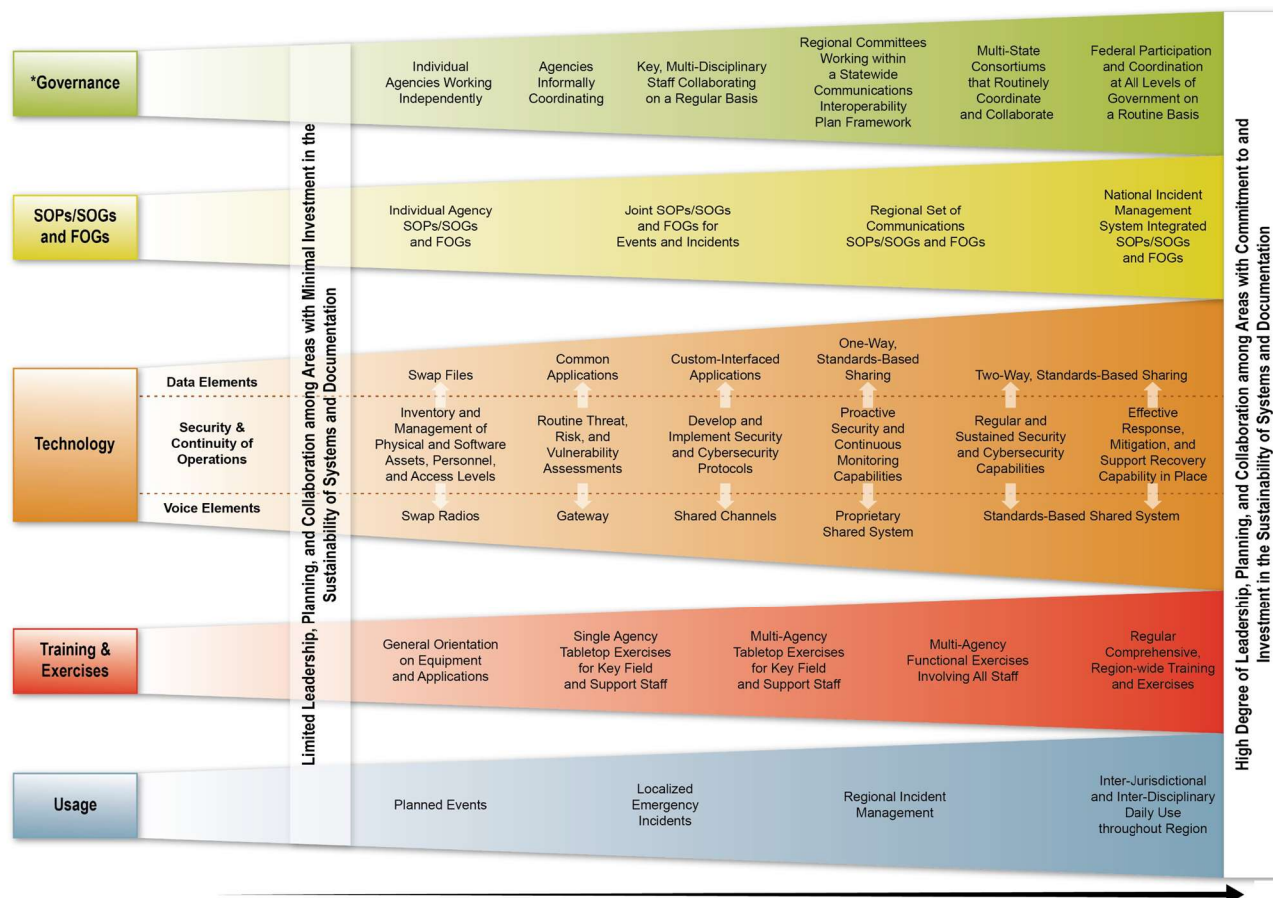


Figure 1: Interoperability Continuum

Interoperability and Emergency Communications Overview

Interoperability is the ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized. Reliable, timely communications among public safety responders and between public safety agencies and citizens is critical to effectively carry out public safety missions, and in many cases, saving lives.

Traditional voice capabilities, such as land mobile radio (LMR) and landline 911 services, have long been and continue to be critical tools for communications. However, the advancement of internet protocol-based technologies in public safety has increased the type and amount of information responders receive, the tools they communicate with, and complexity of new and interdependent systems. Emerging technologies increase the need for coordination across public safety disciplines,

² [Interoperability Continuum Brochure](#)

communications functions, and types of government agencies to ensure emergency communications capabilities are interoperable, reliable, and secure.

An example of this evolution is the transition of public-safety answering points (PSAPs) to Next Generation 911 (NG911) technology that will enhance sharing of critical information in real-time using multimedia—such as pictures, video, and text—among citizens, PSAP operators, dispatchers, and first responders. While potential benefits of NG911 are tremendous, implementation challenges remain. Necessary tasks to fully realize these benefits include interfacing disparate systems, developing training and standard operating procedures (SOPs), and ensuring information security.

VISION AND MISSION

This section describes Missouri’s vision and mission for improving emergency and public safety communications interoperability.

Vision:

Achieve resilient and secure operable and interoperable communications across the state of Missouri.

Mission:

Partner with all disciplines and jurisdictions to promote and achieve resilient and secure operable and interoperable communications through inclusive governance, developing and implementing standards and best practices, conducting training and exercises, supporting existing while exploring new technologies, and pursuing and securing adequate funding.

GOVERNANCE

Executive Order 06-23 created the Missouri Statewide Interoperability Executive Committee (SIEC).³ The purpose of the SIEC is to develop a statewide communications strategic plan, including but not limited to:

- A statewide interconnected radio system with consolidated state voice dispatch operation;
- Consolidated administration and technical support;
- Advanced communication training; and
- Nationally accepted standards to implement the communications capabilities and procedures required to provide Missouri’s first responders and critical infrastructure community the communications services needed to protect the state’s citizens.

The 10-member voting committee includes representatives from the following entities:

- Missouri’s three largest urban areas – St. Louis, Kansas City, and Springfield;
- Rural areas of the state – north, central, and south/southeast;

³ [Missouri Executive Order 06-23, 2006](#)

- The three largest state government radio systems – the Departments of Transportation, Conservation, and Public Safety; and
- Missouri’s critical infrastructure and utility community.

The SIEC is under the authority of the Homeland Security Advisory Council (HSAC).⁴ The Missouri Department of Public Safety (DPS) Director or his designee chairs the SIEC. Currently, the SWIC is the SIEC chair as a designee. The SIEC cannot enforce policies but serves as an advisory board for the Missouri Statewide Interoperable Network (MOSWIN)⁵ and interoperability guidelines in general.

As part of the SCIP development process, webinars were held where Missouri stakeholders identified various interoperability challenges, emerging issues, risks and threats, and desired states across the emergency communications ecosystem. Based upon stakeholder feedback, goals and objectives were developed to help focus efforts, resources, and funding over the next three years.

The **challenges** identified during the SCIP process highlight a significant need for consistency in participation and knowledge retention within Missouri’s statewide emergency communication systems. The turnover of personnel leads to a loss of expertise, particularly impacting local agencies’ understanding of radio operations and interoperability processes. Vacancies within the SIEC and the lack of a formal process for filling these positions have further hindered representation and coordination. Agencies vary in terms of training, staffing, and priority on system education, contributing to inefficiencies in communication. Enhanced information-sharing mechanisms are necessary, with home-rule limitations making stakeholder engagement difficult.

Emerging issues, such as encryption-related conflicts in trust environments and potential malicious attacks on physical security systems, pose considerable risks to the system’s overall functionality and interoperability. Additionally, a lack of focus on contingency planning could exacerbate these vulnerabilities. Risk factors include shifting public sentiment towards public safety and the potential impacts of artificial intelligence (AI), which presents both risks and opportunities for the emergency communication infrastructure.

The **desired states** call for the development of a comprehensive regional and statewide interoperability plan to ensure seamless communication across agencies during routine operations, special events, and emergency situations. Additionally, it is critical to expand governance to encompass the full communications cycle, ensuring holistic oversight. The SIEC should streamline the process for filling vacant positions in a timelier manner, with the body potentially leading this effort. Furthermore, clear procedures for submitting issues or proposals to the SIEC should be established to enhance efficiency and responsiveness.

Missouri’s emergency communications governance map is depicted in Figure 2, below.

⁴ [Missouri Executive Order 06-23, 2006](#)

⁵ [MOSWIN - Missouri Interoperable Communications](#)

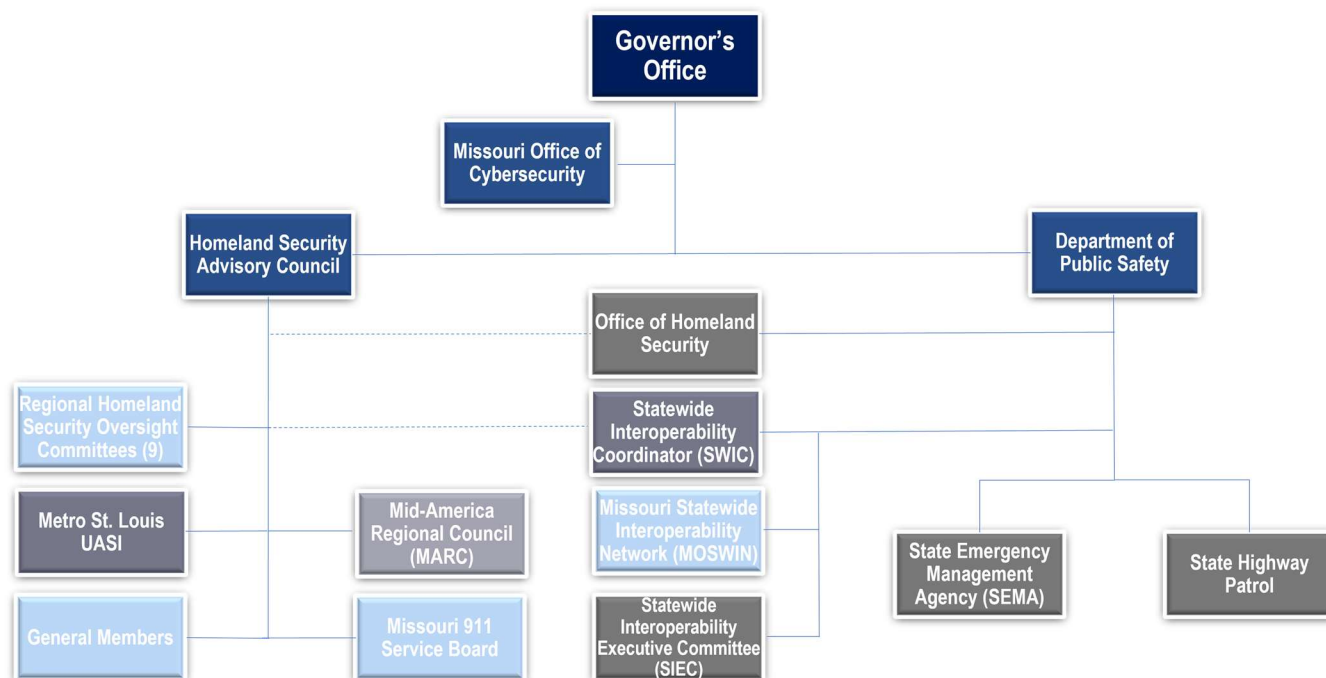


Figure 2: Missouri's Emergency Communications Governance Map

Governance goals and objectives include the following.

Governance	
Goals	Objectives
1. Expand participation in statewide communications planning and governance	1.1 Encourage participation from all public safety lanes of communication in the Statewide Interoperability Executive Committee (SIEC) (i.e., land mobile radio [LMR], 911 Service Board, alerts and warnings, broadband, cybersecurity, etc.)
	1.2 Develop governance policies for interworking of LMR and broadband
	1.3 Clarify the role of the SIEC including what it does, what it was made for, etc.
2. Encourage regions to review, de-conflict, and update their regional communication plans	2.1 Coordinate resources, training, and guidance for communications planning
	2.2 Identify sustainable funding streams
	2.3 Update and disseminate regional Tactical Interoperable Communications Plans (TICPs) and Field Operations Guides (FOGs)
3. Support regional and state-level interoperable communications trainings and exercises	3.1 Support local Communications Unit Exercise (COMMEX) events
	3.2 Exercise and evaluate people, procedures, and equipment
	3.3 Refine and disseminate best practices
	3.4 Increase user and refresher training options
	3.5 Support Communications Unit (COMU) and Information and Communications Technology (ICT) positions
	3.6 Support and increase awareness of the COMU Recognition Standard Operating Procedure (SOP)

Goals	Objectives
	3.7 Facilitate the delivery of communication-related ICT courses at the local and state levels
4. Develop a comprehensive outreach and information-sharing plan to enhance interoperable communications	4.1 Identify, create, and maintain a Statewide Interoperability Coordinator (SWIC) outreach tool (portal, newsletter, etc.)
	4.2 Create a central repository to help disseminate information and materials
	4.3 Disseminate guidelines and best practices for secure communications (i.e., encryption, cybersecurity, etc.)

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

Missouri has built a statewide public safety interoperable communications system, known as MOSWIN.⁶ MOSWIN is a network of communications towers, base stations, and communications software. The project builds the infrastructure that will provide interoperable communications throughout the state to both state public safety agencies and any local jurisdictions that wish to use the system for their interoperable communications.

MOSWIN serves two primary functions:

- Providing **internal communications** capabilities for numerous city, county, state, and federal agencies, including law enforcement, fire, emergency medical services, and emergency management and public safety support services; and
- Providing a statewide **interoperability platform** and access for local agencies to achieve interoperable communications with local, state, regional, and federal agencies.

The network operates five or more channels per site in the “trunked” mode and utilizes both Very High Frequency (VHF) High Band public safety spectrum consisting of 75 radio sites statewide, 700 MHz public safety spectrum consisting of 75 radio sites statewide, and 800 MHz public safety spectrum consisting of 30 sites in metropolitan areas.

MOSWIN is designed in accordance with the Association of Public-Safety Communications Officials (APCO) Project 25 (P25) standards for mission-critical public safety radio communications.⁷ P25 radios are required to access MOSWIN for Level 1 (full-time) and Level 2 (interoperability only) member agencies.

There are many disparate public safety LMR systems operating in multiple radio bands throughout Missouri. Each county and city have at least one radio system for police, fire, and emergency medical services (EMS). St. Louis and Kansas City have regional shared systems operating in the 700 Megahertz (MHz) and 800 MHz frequency bands, while most other systems in the state operate in the VHF spectrum. These systems interface with MOSWIN, supported by Memoranda of Understanding (MOUs). Many agencies operate primarily on MOSWIN and maintain their legacy conventional system as a contingency emergency backup.

⁶ [Missouri Interoperable Communications - MOSWIN](#)

⁷ [MOSWIN Policy Title – LTE Network, 2018](#)

Some of the other regional radio systems in the state include the Kansas City Metropolitan Area Regional Radio System (MARRS), the St. Louis Area Trunked Radio System (SLATER), among others. Many of the P25-compatible systems are being integrated with MOSWIN through core connectivity via the Inter-Radio Frequency Subsystem Interface (ISSI).

The challenges identified during the SCIP process related to Missouri's communication systems primarily revolve around rising maintenance costs, limiting the ability to introduce new sites and infrastructure, alongside staff turnover issues that lead to a loss of knowledge within local agencies. User training gaps regarding radio zones, talk group navigation, and overall end-user competency further hinder the effectiveness of communications. The need for connectivity with neighboring states and smaller agencies adds complexity to interoperability efforts. The increasing number of users and encryption support also pose significant challenges.

Emerging issues include the integration of Long-Term Evolution (LTE) into LMR systems, which introduces vulnerabilities and potential cost increases, as well as a more congested radio environment. It opens the door to new threats and dependencies unfamiliar to the state. Risks and threats primarily focus on aging equipment, which affects coverage and performance.

The desired states call for increased outreach efforts to improve familiarity with communication systems and to establish pathways for seamless integration into conventional systems. Efforts to counter misinformation and ensure user ability to move between systems are critical. Promoting the use of dual-band radios and enhancing coverage through best practices are key objectives. Maintaining system availability while enhancing security is a priority, alongside the creation of purchasing guidelines for radios based on best practices. Standardizing talkgroups, optimizing security through remote configuration, and increasing collaboration with the MOSWIN system are also central goals. System owners should retain final authority over the integration of new technologies.

911

The 911 Service Board provides overall 911 governance in the state. The Missouri 911 Service Board consists of 15 members representing 911 experts and represents all Missouri 911 entities and jurisdictions.⁸ Members are appointed by the Governor and confirmed by the Senate. The Board strives toward immediate access to emergency services for all citizens in the state of Missouri. It has the responsibility to assist and advise the state in ensuring the availability, implementation, and enhancement of 911 services common to all jurisdictions through research, planning, training, and education.⁹ The Board receives service grants to help implement NG911 in local and rural areas. The Board is doing an aerial resource assessment and evaluation of the state to help access with geographic information systems (GIS). Additionally, several Emergency Services Internet Protocol Networks (ESInets) have been set up, and the Board is checking for availability.

Missouri does not have a statewide 911 network¹⁰ and the state's approximately 185 independent Emergency Communication Centers (ECCs) manage 911 at the local level, operating under county-level or regional systems. Most counties provide Phase II level service, which helps ECCs locate callers dialing 911 from cell phones, as well as receiving text-to-911. However, some counties lack the ability to geographically locate callers who call from cell phones due to obsolete equipment.

⁸ [Missouri 911 Service Board](#)

⁹ [Missouri 911 Service Board By-Laws, 2020](#)

¹⁰ [Missouri 911 Modernization and Improvement Report, 2017](#)

Many Missouri ECCs rely on antiquated technology and this operations and maintenance of this technology is rapidly becoming unsustainable. A great variance in equipment and technology among Missouri ECCs impedes the interoperability necessary to transfer 911 calls and call-related data (i.e., Automatic Number Identification/Automatic Location Identification (ANI/ALI) to another PSAP).

Missouri is in the process of implementing NG911 in the state. With the establishment of the Statewide 911 Coordinator, collaboration and coordination across the state's independent ECCs has improved. Although all counties have 911 coverage in the state, not all of them are on NG911.

Missouri is continuing to work on the following challenges to implementing NG911 in the state:

- Expansion of NG911 capabilities for remaining counties in Missouri by the end of calendar year 2025 which will provide location data and other modern features;
- Lack of statewide 911 data interoperability across independent ECCs;
- Discrepancies in service level capabilities;
- Inability to geographically locate 911 wireless callers, minimal level of emergency medical dispatch (EMD) services (over half of Missouri ECCs cannot provide EMD services);
- Antiquated and incompatible 911 infrastructure across PSAPs; and
- Understaffed ECCs.

In addition to the above needs, state agencies have committed to support the following initiatives to address 911 service gaps:

- Continue consistent collaboration with the 911 Service Board;
- Expansion of a Statewide ESInet;
- Statewide computer-aided dispatch (CAD) capabilities;
- Consolidation when appropriate and available;
- Statewide GIS mapping to NG911 GIS standards;
- Development of a NG911 Roadmap;
- 911 training standard revision and virtual delivery;
- 911 system redundancy for any technological or disaster incidents that impact PSAPs; and
- Aid underserved PSAPs with broadband efforts.

In connection with the process of implementing NG911 throughout the state, an NG911 Readiness Assessment was completed by an outside consultant in December 2021.¹¹ The resulting report indicated that Missouri is in a transitional stage where the migration to NG911 has begun in some geographic and technical areas. This level of readiness indicates that some technology is already in place and that Missouri is beginning to take the steps toward planning and implementing NG911. Before fully diving into the technical and operational aspects of NG911, many areas still need improvement.

The **challenges** identified during the SCIP process include statewide inconsistencies in the availability of services such as text-to-911, as well as varying levels of technology dependency. Call-taking scripts are not uniformly documented, and information sharing is limited or filtered across agencies. The continued use of 10-codes by some agencies creates confusion, while disparate service providers hinder the seamless transfer of calls between ECCs. Additionally, fiber cuts lead to service disruptions, prompting a need for status monitoring programs to manage outages. **Emerging issues**

¹¹ [NG911 Readiness Assessment Report, 2021](#)

include the increasing risk of information overload and the ongoing evolution and implementation of NG911 technology, which presents both opportunities and challenges.

Broadband

With the build-out of broadband in the state, Missouri plans to implement standards for broadband roaming and interoperability tool usage between disparate carriers. Further, the re-investment in broadband presents an opportunity to develop interworking functions between broadband and LMR and to leverage broadband build-out with LMR built-out. State agencies and system owners will continue to exercise governance and provide input over LMR to LTE solutions and support the development of a must-carry talk group for interoperability.

Missouri opted into FirstNet in 2017. The state seeks to develop a FirstNet re-investment plan with stakeholder input and to educate stakeholders on FirstNet-provided tools via workshops and virtual engagements. The state has already begun to partner with FirstNet to develop virtual resources.

MOSWIN System Administration recognizes public safety broadband is an emerging technology that can enhance public safety interoperable communications.¹² Level 1 and Level 2 Member Agencies are permitted to interface public safety broadband to MOSWIN upon MOSWIN System Administration approval. Only the DPS MOSWIN System Administration can/will approve public safety broadband interfaces. Additionally, MOSWIN agencies seeking to connect broadband LTE push-to-talk (PTT) functionality to the MOSWIN network must obtain approval from the MOSWIN System Administration regardless of the broadband PTT service or application(s) utilized.

Currently, SmartConnect allows radios to access the system through LTE and Wi-Fi. The state is researching other broadband interface options.

The **challenges** identified during the SCIP process emphasize the need for improved connectivity and the complexities associated with maintaining local control over communication systems. There is a significant reliance on commercial vendors, which introduces concerns regarding both security and cost. Public safety agencies have limited influence on what technologies vendors use to secure their systems, how often they are updated, and must anticipate regular service fee increases from those vendors, all of which leave agencies vulnerable due to lack of control over commercial and private infrastructure. **Emerging issues** include the potential for AI to be exploited as a tool for disruption, posing new risks to communication infrastructure and security.

The **desired states** focus on developing interworking functions between broadband and LMR systems to enhance communication capabilities. There is a need to manage expectations regarding the functionalities and limitations of these systems. Additionally, carrier interoperability must be established for areas with limited coverage. The development of governance policies to guide the integration of LMR and broadband systems is also essential to ensure seamless and coordinated operations.

Alerts and Warnings

In Missouri, most alerts and warnings come from local agencies, many of whom have their own private alerting systems. There is no statewide alerts and warnings plan, and Emergency Support Function 2 (ESF-2) teams do not have access to information on messaging capabilities for each locality. The state plans to increase utilization of the FEMA Integrated Public Alerts and Warnings

¹² [MOSWIN Policy Title – LTE Network, 2018](#)

System (IPAWS) and other alerting systems statewide as well as create an automated transfer of statewide alerts to the local level. Additionally, Missouri plans to establish a messaging strategy for connectivity outages and develop a mechanism to counter misinformation established by social media platforms. An SOP has been drafted and efforts are ongoing for finalization, adoption, and maintenance.

Currently, Missouri has 10 IPAWS alerting authorities across the state.¹³ The state utilizes tornado sirens and National Oceanic and Atmospheric Administration (NOAA) All-Weather Radios to alert the public of weather-related incidents.¹⁴ Additionally, Missouri residents are encouraged to register for additional alerts through their local governments and media outlets.

During the SCIP process, it was identified that there are multiple applications and methods for getting information out, but there are no standard plans for usage. The **desired states** emphasize the need for the development of a clear framework for the Emergency Alert System (EAS). This includes expanding and implementing IPAWS launch authorities and establishing a consistent policy for valid messaging through IPAWS. Additionally, it is important to designate clear initiation points for messaging to ensure uniformity and effectiveness in alert dissemination.

Cybersecurity

To document Missouri cybersecurity goals and strategies, the Office of Cybersecurity (OCS) developed and published their Fiscal Year 2020 Cyber Security Plan.¹⁵ Missouri's vision for cybersecurity has state agencies doing most of their business electronically under conditions of acceptable risk to state assets.

The goals from this plan include:

- Create a culture that fosters the adoption of cybersecurity best practices;
- Use cutting-edge technology to protect state assets;
- Respond to cybersecurity incidents swiftly and effectively; and
- Establish and maintain IT governance that promotes cybersecurity.

Additionally, the Mid-America Regional Council (MARC) helped facilitate the creation of a Regional Cybersecurity Strategic Framework to strengthen the capacity of local governments to address cybersecurity threats in a coordinated effort.¹⁶ The Framework was created by the Regional Homeland Security Coordinating Committee and a planning team of city and county leaders, information technology (IT) professionals, emergency managers, and cybersecurity experts.

The Framework outlines six targeted actions that MARC and the region could implement to achieve the shared vision of reducing cybersecurity threats:

1. Identify and establish best practices for cybersecurity planning;
2. Design and implement regional communication strategies;
3. Create collaborative training opportunities to build a high-quality workforce;
4. Create a shared services model to support local governments;
5. Improve redundancy and resilience through mutual aid networks and shared services; and

¹³ [IPAWS Alerting Authorities](#)

¹⁴ [Missouri Storm Aware](#)

¹⁵ [Missouri Cyber Security Plan, 2020](#)

¹⁶ [MARC – Cybersecurity](#)

6. Establish a sustainable funding source to support regional response to cyber threats.

Some areas of Missouri have begun to proactively evaluate their cybersecurity posture. The state recently supported a Cybersecurity and Infrastructure Security Agency's (CISA) assessment on the SLATER radio system. SLATER agencies and the state were provided recommendations to review based on this assessment.

The primary **challenges** identified during the SCIP process revolve around maintaining operational continuity while upholding security standards. **Emerging issues** include the need to keep technology updated to counter evolving cyber threats and the growing necessity for personnel dedicated to managing public safety systems. Moreover, there is a call for regularly updated and exercised cyber response plans, particularly as AI introduces new complexities. **Threats and risks** include increased vulnerability to cyberattacks, ransom demands, and potential security risks posed by foreign-made equipment. The sector must address the impact of cloud migration and the evolving nature of cybersecurity threats posed by extremist groups. There is a **desire** to monitor the demarcation points and maintain the ability to secure a zone or a system on the fly as needed in the event of a threat between all systems and platforms.

Technology and cybersecurity goals and objectives include the following:

Technology and Cybersecurity	
Goals	Objectives
5. Explore and implement interoperability solutions with disparate systems	5.1 Maintain current Inter Radio Frequency Subsystem Interface (ISSI) connections
	5.2 Pursue opportunities for increased inter-system connections
	5.3 Collaborate with disparate systems to implement interoperability solutions
	5.4 Collaborate with bordering states to link systems and share interoperable resources
	5.5 Coordinate and manage broadband solutions
	5.6 Manage patching of disparate systems
6. Improve Missouri's Statewide Interoperable Network (MOSWIN) coverage, capacity, security, and resilience	6.1 Support local investment to enhance the system
	6.2 Add sites and channels to improve coverage and capacity
	6.3 Enhance backhaul technology options (i.e., satellite, Long Term Evolution [LTE], fiber, microwave, etc.)
	6.4 Coordinate system stakeholder implementation of bi-directional amplifier (BDA) systems and incorporate best practices
7. Support the 911 Service Board's efforts to implement Next Generation 911 (NG911) statewide	7.1 Support 911 services board as they develop, sustain, and connect regional Emergency Services Internet Protocol Networks (ESInets)
	7.2 Support development of best practices or standards for call processing
	7.3 Explore the capability to monitor the status of Emergency Communication Centers (ECCs) and Public Safety Answering Points (PSAPs)
8. Support formalized management of Integrated Public Alerts and Warnings System (IPAWS) and other alerting systems statewide	8.1 Develop the framework for consistent statewide alert and warning protocols
	8.2 Work towards formalizing and expanding IPAWS launch authority
	8.3 Support development of multilingual alerts deliveries

Goals	Objectives
9. Manage broadband and LMR interworking functions	9.1 Develop policies for interworking of LMR and broadband
	9.2 Develop functions and manage expectations for LMR and broadband interworking
	9.3 Monitor application-level interoperability between carriers
10. Develop collection of best practices for communications cybersecurity	10.1 Align communications cybersecurity with data cybersecurity guidelines
	10.2 Develop a set of best practices that captures needs and recommendations
	10.3 Increase cybersecurity training for public safety users
	10.4 Maintain awareness of emerging cybersecurity threats to communications
	10.5 Develop strategies to isolate system segments when vulnerabilities are identified

FUNDING

A 3% 911 wireless surcharge is implemented in nearly all counties. Provisions for the prepaid wireless surcharge include a portion of the 3% funds being returned to the county, and the first \$15 of any prepaid charge being exempt from fees. In counties that impose a 911 sales tax, prepaid purchases are exempt from the tax and instead are subject to the 3% fee.

Prepaid cell phone funding can be leveraged by counties in need of NG911 expansion. Funding for 911 expansion has also been allocated through the American Rescue Plan Act (ARPA), but this is a short-term provision rather than an ongoing one.

Adequate funding exists to continue the expansion of the MOSWIN system, although this expansion has also resulted in increased costs due to additional equipment, rising leasing fees, and inflation. Current funding sources for radios include the Local Law Enforcement Block Grant, the Homeland Security Grant Program, and the State and Local Cybersecurity Grant Program. Additionally, a grant requirement mandates that MOSWIN radios must be dual-band capable.

Challenges identified during the SCIP process include securing ongoing funding sources for the phased statewide implementation of NG911, as reliance on 911 Board trust funds is unsustainable. Although grants are available to assist agencies in transitioning to NG911, these efforts result in an interconnected system rather than a unified statewide solution. Additionally, challenges arise from difficulties in transferring county tax revenues to cities for 911, implementing 911-related taxes, and sustaining operational funding. Staffing issues persist due to the need for recovery from Covid-related understaffing and the demands of emerging technologies. The state also faces increasing costs due to reliance on leased spaces, inflation affecting equipment acquisition, and the fiscal challenge of integrating LTE systems with LMR. Smaller and rural areas struggle with the cost of entry into radio systems, and coordinating budgets across counties remains complex.

Emerging issues include keeping technology updated to address cyber threats and the fast-evolving technology ecosystem. Aging equipment is nearing the end of its lifecycle, requiring new funding streams for replacement. Platform changes, while necessary, are costly and may not receive approval due to budgetary constraints. **Threats and risks** include the continued challenge of supporting existing systems amidst limited budgets and inflation, as well as the increasing threat of cyberattacks that could result in ransom demands and service disruptions. There is a **desire** to educate key decision makers on the need, cost, and essential nature of public safety needs.

Funding goals and objectives include the following:

Funding	
Goals	Objectives
11. Maintain sustainability funding to support MOSWIN – Statewide Interoperable Radio Platform	11.1 Sustain capital improvements and operating costs
	11.2 Research sustainable funding avenues for MOSWIN LMR lifecycle replacement
	11.3 Develop and maintain supporting materials and information that can be used when talking about public safety needs (i.e., LMR, NG911, public safety broadband, alerts and warnings, etc.)

IMPLEMENTATION PLAN

Each goal and its associated objectives have a timeline with a target completion date, and one or multiple owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require the support and cooperation from numerous individuals, groups, or agencies, and will be added as formal agenda items for review during regular governance body meetings. CISA's ICTAP has a catalog¹⁷ of technical assistances (TAs) available to assist with the implementation of the SCIP. TA requests are to be coordinated through the SWIC.

Missouri's implementation plan is shown in the table below.

Goals	Objectives	Owners	Completion Dates
1. Expand participation in statewide communications planning and governance	1.1 Encourage participation from all public safety lanes of communication in the Statewide Interoperability Executive Committee (SIEC) (i.e., land mobile radio [LMR], 911 Service Board, alerts and warnings, broadband, cybersecurity, etc.)	SWIC SIEC	1.1 Ongoing
	1.2 Develop governance policies for interworking of LMR and broadband		1.2 Q4 2025
	1.3 Clarify the role of the SIEC (what it does, what it was made for, etc.)		1.3 Q4 2025
2. Encourage regions to review, de-conflict, and update their regional communication plans	2.1 Coordinate resources, training, and guidance for communications planning	SWIC SIEC	Ongoing
	2.2 Identify sustainable funding streams		
	2.3 Update and disseminate regional Tactical Interoperable Communications Plans (TICPs) and Field Operations Guides (FOGs)		
3. Support regional and state-level interoperable communications trainings and exercises	3.1 Support local Communications Unit Exercise (COMMEX) events	SWIC SIEC STO	Ongoing
	3.2 Exercise and evaluate people, procedures, and equipment		
	3.3 Refine and disseminate best practices		
	3.4 Increase user and refresher training options		
	3.5 Support Communications Unit (COMU) and Information and Communications Technology (ICT) positions		
	3.6 Support and increase awareness of the COMU Recognition Standard Operating Procedure (SOP)		

¹⁷ [Emergency Communications Technical Assistance Planning Guide](#)

Goals	Objectives	Owners	Completion Dates
	3.7 Facilitate the delivery of communication-related ICT courses at the local and state levels		
4. Develop a comprehensive outreach and information-sharing plan to enhance interoperable communications	4.1 Identify, create, and maintain a Statewide Interoperability Coordinator (SWIC) outreach tool (portal, newsletter, etc.)	SWIC DPS	Q4 2025
	4.2 Create a central repository to help disseminate information and materials		
	4.3 Disseminate guidelines and best practices for secure communications (i.e., encryption, cybersecurity, etc.)		
5. Explore and implement interoperability solutions with disparate systems	5.1 Maintain current Inter Radio Frequency Subsystem Interface (ISSI) connections	All System Owners	Ongoing
	5.2 Pursue opportunities for increased inter-system connections		
	5.3 Collaborate with disparate systems to implement interoperability solutions		
	5.4 Collaborate with bordering states to link systems and share interoperable resources		
	5.5 Coordinate and manage broadband solutions		
	5.6 Manage patching of disparate systems		
6. Improve Missouri's Statewide Interoperable Network (MOSWIN) coverage, capacity, security, and resilience	6.1 Support local investment to enhance the system	MOSWIN Zone Partners	Ongoing
	6.2 Add sites and channels to improve coverage and capacity		
	6.3 Enhance backhaul technology options (i.e., satellite, Long Term Evolution [LTE], fiber, microwave, etc.)		
	6.4 Coordinate system stakeholder implementation of bi-directional amplifier (BDA) systems and incorporate best practices		
7. Support the 911 Service Board's efforts to implement Next Generation 911 (NG911) statewide	7.1 Support 911 services board as they develop, sustain, and connect regional Emergency Services Internet Protocol Networks (ESInets)	SWIC SIEC	Ongoing
	7.2 Support development of best practices or standards for call processing		
	7.3 Explore the capability to monitor the status of Emergency Communication Centers (ECCs) and Public Safety Answering Points (PSAPs)		
8. Support formalized management of Integrated Public Alerts and	8.1 Develop the framework for consistent statewide alert and warning protocols	SIWC SIEC DPS	Q2 2026
	8.2 Work towards formalizing and expanding IPAWS launch authority		

Goals	Objectives	Owners	Completion Dates
Warnings System (IPAWS) and other alerting systems statewide	8.3 Support development of multilingual alerts deliveries		
9. Manage broadband and LMR interworking functions	9.1 Develop policies for interworking of LMR and broadband	SWIC SIEC Zone Partners Broadband and LMR Vendors	Ongoing
	9.2 Develop functions and manage expectations for LMR and broadband interworking		
	9.3 Monitor application-level interoperability between carriers		
10. Develop collection of best practices for communications cybersecurity	10.1 Align communications cybersecurity with data cybersecurity guidelines	SIEC Office of Homeland Security CISA Communications Vendors MOSWIN Zone Partners CJIS OAITSD	Ongoing
	10.2 Develop a set of best practices that captures needs and recommendations		
	10.3 Increase cybersecurity training for public safety users		
	10.4 Maintain awareness of emerging cybersecurity threats to communications		
	10.5 Develop strategies to isolate system segments when vulnerabilities are identified		
11. Maintain sustainability funding to support MOSWIN – Statewide Interoperable Radio Platform	11.1 Sustain capital improvements and operating costs	SWIC SIEC DPS MOSWIN Zone Partners	Ongoing
	11.2 Research sustainable funding avenues for MOSWIN LMR lifecycle replacement		
	11.3 Develop and maintain supporting materials and information that can be used when talking about public safety needs (i.e., LMR, NG911, public safety broadband, alerts and warnings, etc.)		

APPENDIX A: STATE MARKERS

In 2019, CISA supported states and territories in establishing an initial picture of interoperability nationwide by measuring progress against 30 markers. These markers describe a state or territory's level of interoperability maturity. Below is Missouri's assessment of their progress against the markers as of March 2025.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
1	State-level Emergency Communications Governing Body Established (e.g., SIEC, SIGB): Governance framework is in place to sustain all emergency communications.	Emergency communications governing body does not exist, or exists but the body has not been formalized by legislative or executive actions.	Emergency communications governing body is established through an executive order	Emergency communications governing body is condified through a state law
2	Emergency Communications Governing Body Inclusion: Statewide governance body is comprised of all components of the emergency communications ecosystem (Communication Champion/SWIC, LMR, Broadband/LTE, 911, and AWN) and invites other relevant emergency communications partners to participate in the meetings.	Initial (1-5) Governance body participation includes: <input type="checkbox"/> Communications Champion/SWIC <input type="checkbox"/> LMR <input type="checkbox"/> Broadband/LTE <input type="checkbox"/> 911 <input type="checkbox"/> Alerts, Warnings, and Notifications <input type="checkbox"/> Federal components representatives <input type="checkbox"/> CISA (ECC, CSA, etc.) <input type="checkbox"/> Federal Law Enforcement <input type="checkbox"/> Federal Land Management <input type="checkbox"/> FEMA <input type="checkbox"/> US Dept. of Health and Human Services <input type="checkbox"/> Military (including Coast Guard) <input type="checkbox"/> State Cyber Representatives <input type="checkbox"/> State Chief Information Officer <input type="checkbox"/> State Legislative Liaison <input type="checkbox"/> State Emergency Management Agency <input type="checkbox"/> State Homeland Security Advisor or representative	Defined (6-10) Governance body participation includes: <input type="checkbox"/> Communications Champion/SWIC <input type="checkbox"/> LMR <input type="checkbox"/> Broadband/LTE <input type="checkbox"/> 911 <input type="checkbox"/> Alerts, Warnings, and Notifications <input type="checkbox"/> Federal components representatives <input type="checkbox"/> CISA (ECC, CSA, etc.) <input type="checkbox"/> Federal Law Enforcement <input type="checkbox"/> Federal Land Management <input type="checkbox"/> FEMA <input type="checkbox"/> US Dept. of Health and Human Services <input type="checkbox"/> Military (including Coast Guard) <input type="checkbox"/> State Cyber Representatives <input type="checkbox"/> State Chief Information Officer <input type="checkbox"/> State Legislative Liaison <input type="checkbox"/> State Emergency Management Agency <input type="checkbox"/> State Homeland Security Advisor or representative	Optimized (10+) Governance body participation includes: <input checked="" type="checkbox"/> Communications Champion/SWIC <input checked="" type="checkbox"/> LMR <input checked="" type="checkbox"/> Broadband/LTE <input checked="" type="checkbox"/> 911 <input checked="" type="checkbox"/> Alerts, Warnings, and Notifications <input checked="" type="checkbox"/> Federal components representatives <input checked="" type="checkbox"/> CISA (ECC, CSA, etc.) <input checked="" type="checkbox"/> Federal Law Enforcement <input type="checkbox"/> Federal Land Management <input checked="" type="checkbox"/> Federal Emergency Management Agency <input checked="" type="checkbox"/> US Dept. of Health and Human Services <input type="checkbox"/> Military (including Coast Guard) <input type="checkbox"/> State Cyber Representatives <input checked="" type="checkbox"/> State Chief Information Officer <input checked="" type="checkbox"/> State Legislative Liaison <input checked="" type="checkbox"/> State Emergency Management Agency

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
		<input type="checkbox"/> State Administrative Agency Representative <input type="checkbox"/> National Guard <input type="checkbox"/> Local or County Representatives <input type="checkbox"/> Tribal Representatives <input type="checkbox"/> Other (Please Specify)	<input type="checkbox"/> State Administrative Agency Representative <input type="checkbox"/> National Guard <input type="checkbox"/> Local or County Representatives <input type="checkbox"/> Tribal Representatives <input type="checkbox"/> Other (Please Specify)	<input type="checkbox"/> State Homeland Security Advisor or representative <input type="checkbox"/> State Administrative Agency Representative <input checked="" type="checkbox"/> National Guard <input checked="" type="checkbox"/> Local or County Representatives <input type="checkbox"/> Tribal Representatives <input type="checkbox"/> Other (Please Specify)
3	SWIC Position Established: A full-time employee, either a SWIC or an employee that performs the duties of a SWIC, is in place to promote the performance of all Interoperability Markers	A SWIC position or an employee performing the duties of the SWIC position does not exist	A full-time SWIC position with collateral duties or a full-time employee with the duties of the SWIC position as part of their collateral duties. Also, the SWIC position appears in the Administrative Rule of the state/territory agency that the SWIC serves in or is established through Executive Order.	A full-time SWIC position established through state law

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
4	SWIC Office established: The SWIC has a dedicated office, that includes a deputy SWIC and support staff	A SWIC, or full-time employee performing the duties of a SWIC as collateral duties, is the only person in place to promote the performance of all Interoperability Markers	A SWIC and deputy SWIC are the only two people in place to promote the performance of all Interoperability Markers	A SWIC has a deputy SWIC as well as one or more additional full-time employee/s in place to promote the performance of all Interoperability Markers
5	SWIC and/or SWIC Office State/Territory Level Coordination: A state/territory coordination across all emergency communications technologies is at the core of successful emergency communications interoperability. If the SWIC and/or SWIC office is not the primary lead for a specific governance, policy, technology, training & exercise, or usage role, the SWIC and/or SWIC office should play a significant coordinating role in bringing the responsible leads together to further enhance a state or territory ability to improve interoperable emergency communications.	The SWIC and/or its office has coordinated with 1-4 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state/territory level (check all that apply): <input type="checkbox"/> 911-Telephone, CAD, and NG911 <input type="checkbox"/> Governance <input type="checkbox"/> Training and Exercises <input type="checkbox"/> Cybersecurity <input type="checkbox"/> Radio Communications Systems <input type="checkbox"/> Broadband and Data Systems <input type="checkbox"/> Alerts and Warnings <input type="checkbox"/> State-level Emergency Management Agency <input type="checkbox"/> Priority Telecommunications Services <input type="checkbox"/> UASI Involvement <input type="checkbox"/> Tribal Engagement <input type="checkbox"/> IMT Coordinator	The SWIC and/or its office has coordinated with 5-8 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state/territory level (check all that apply): <input type="checkbox"/> 911-Telephone, CAD, and NG911 <input type="checkbox"/> Governance <input type="checkbox"/> Training and Exercises <input type="checkbox"/> Cybersecurity <input type="checkbox"/> Radio Communications Systems <input type="checkbox"/> Broadband and Data Systems <input type="checkbox"/> Alerts and Warnings <input type="checkbox"/> State-level Emergency Management Agency <input type="checkbox"/> Priority Telecommunications Services <input type="checkbox"/> UASI Involvement <input type="checkbox"/> Tribal Engagement <input type="checkbox"/> IMT Coordinator	The SWIC and/or its office has coordinated with 9-12 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state level (check all that apply): <input checked="" type="checkbox"/> 911-Telephone, CAD, and NG911 <input checked="" type="checkbox"/> Governance <input checked="" type="checkbox"/> Training and Exercises <input checked="" type="checkbox"/> Cybersecurity <input checked="" type="checkbox"/> Radio Communications Systems <input checked="" type="checkbox"/> Broadband and Data Systems <input checked="" type="checkbox"/> Alerts and Warnings <input checked="" type="checkbox"/> State-level Emergency Management Agency <input checked="" type="checkbox"/> Priority Telecommunications Services <input checked="" type="checkbox"/> UASI Involvement <input type="checkbox"/> Tribal Engagement <input type="checkbox"/> IMT Coordinator
6	Statewide Communication Interoperability Plan (SCIP) Refresh: SCIP is a planning document that continues to be executed in a timely manner. Updated SCIPs are reviewed and approved by SIGB/SIEC.	The state/territory does not have a SCIP	The state/territory has a SCIP, but it is older than three years	The state/territory has a SCIP that has been updated within the past three years.
7	Completion of SCIP goals: The state/territory is on track to accomplish the goals laid out in the SCIP and/or has completed the goals within the desired timeframe	<50% of the SCIP goals are completed or on track for completion	>51%<79% of the SCIP goals are completed or on track for completion	>80% of the SCIP goals are completed or on track for completion

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
8	Utilization of the Emergency Communications Governing Body to discuss SCIP Progress: SCIP progress updates are a regular topic for discussion during for emergency communications governing body meetings.	SCIP progress updates are not included as a meeting agenda topic for the emergency communications governing body meetings	SCIP progress updates are included one to two times a year as a meeting agenda topic for the emergency communications governing body meetings	SCIP progress updates are regularly included as a meeting agenda topic for the emergency communications governing body meetings
9	Integrated Emergency Communication Grant Coordination: For Federal grants funds, the state / territory is tracking and optimizing emergency communications grant proposals with the assistance of the SWIC to ensure compliance and interoperability with national and state/territory standards, alignment with the SCIP, and there is strategic visibility into how grant money is being spent.	No explicit approach or only informal emergency communications grant coordination between localities, agencies, SAA and/or the SWIC within a state / territory	SWIC and/or the emergency communications governing body provides guidance to agencies and localities for emergency communications grant funding but does not review proposals or make recommendations	SWIC and/or the emergency communications governing body provides guidance to agencies and localities for emergency communications grant funding and reviews grant proposals for alignment with the SCIP and complies with appropriate standards such as P25. SWIC and/or the emergency communications governing body provides recommendations to the SAA.
10	TICP (or equivalent) Developed: Tactical Interoperable Communications Plans (TICPs) are established at the statewide or regional level and are periodically reviewed, validated, and updated (if needed). TICPs are socialized with the appropriate public safety stakeholders and are used during exercises.	No statewide or regional TICP in place	Statewide or Regional TICP(s) have been reviewed, validated, and updated (if needed) within the past 2-5 years but has not been socialized with the appropriate public safety stakeholders or used during exercises	Statewide or Regional TICP(s) have been reviewed, validated, and updated (if needed) within the past 2 years and has been socialized with the appropriate public safety stakeholders and are used during exercises
11	Field Operations Guides (FOGs) Developed: Field Operations Guides are established at the statewide or regional level and are periodically reviewed, validated, and updated (if needed). FOGs are socialized with the appropriate public safety stakeholders and are used during exercises	No statewide or regional FOG in place	Statewide or regional FOG(s) have been reviewed, validated, and updated (if needed) within the past 2-5 years but has not been socialized with the appropriate public safety stakeholders or used during exercises	Statewide or regional FOG(s) have been reviewed, validated, and updated (if needed) within the past 2 years and has been socialized with the appropriate public safety stakeholders and are used during exercises
12	Statewide AWN plan: State/Territory has a statewide Alerts, Warnings, and Notifications plan that highlights the roles and responsibilities of each relevant entities.	No statewide or territory-wide AWN plan	Statewide or territory-wide coordinated AWN plan is in place and is older than 2 years	Statewide or territory-wide coordinated AWN plan is in place and has been reviewed within the last 2 years and describes how all Alerts, warnings and notifications are handled across all alerting authorities.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
13	Outreach to Entities not covered in AWN plan: State/Territory understand and know who is not covered by the statewide/territory-wide AWN plan and has an outreach plan in place to build partnerships with these entities.	State/Territory knows which entities are not covered in the statewide/territory-wide AWN plan but has not conducted outreach to such entities	State/Territory knows which entities are not covered in the statewide/territory-wide coordinated AWN plan and has conducted outreach to such entities	State/Territory knows which entities are not covered in the statewide/territory-wide coordinates AWN plan, conducted outreach to such entities, and have incorporated these entities into the overall statewide / territory-wide coordinated plan (e.g., MOU)
14	Radio Programming: State-owned/state-controlled radios are programmed for National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state / territory.	<49% of state-owned/state-controlled radios are programed for interoperability and consistency	>50%<74% of state-owned/state-controlled radios are programed for interoperability and consistency	>75%<100% of state-owned/state-controlled radios are programmed for interoperability and consistency
15	Sustainment of Radio Programming: State/Territory has a radio programming plan developed to ensure radios are programmed for National/Federal, SLTT interoperability channels and channel nomenclature are consist across a state/territory	State/Territory has a radio programming plan or are in the process of developing a radio programming plan	State/Territory has a radio programming plan in place and provide trainings to the radio users to help with compliance	State/Territory has a radio programming plan, provides training to the radio users, and has a sustainability mechanism in place.
16	Continuous Education of Radio Programming: State/Territory has a plan in place to continuously educate radio users on National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state/territory	There is no plan in place for continuous education for radio users on radio programming and channel nomenclature	State/Territory is developing a continuous education plan for radio users on radio programming and channel nomenclature	State/Territory has a continuous education plan in place for radio users on radio programming and channel nomenclature
17	Radio Encryption Plan: The state/territory has an encryption plan that promotes Advanced Encryption Standard (AES) in place for the radio systems within the state/territory	There is no encryption plan that promotes AES in place for the radio systems within the state/territory	The state/territory is developing an encryption plan that promotes AES for radio systems within the state/territory	The state/territory has an encryption plan that promotes AES in place for radio systems within the state/territory

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
18	Cybersecurity Assessment Awareness: Public safety communications network owners have conducted a cybersecurity assessment and developed a cyber incident response plan.	Public safety communications network owners, specifically LMR, 911, and A&W, have completed a cyber security assessment. (check the box by for the public safety communication networks that completed a cybersecurity assessment) <input type="checkbox"/> LMR <input type="checkbox"/> 911 <input type="checkbox"/> Alerts and Warnings	Public safety communications network owners, specifically LMR, 911, and A&W, have completed a cyber security assessment. (check the box by for the public safety communication networks that completed a cybersecurity assessment) <input type="checkbox"/> LMR <input type="checkbox"/> 911 <input type="checkbox"/> Alerts and Warnings	Public safety communications network owners, specifically LMR, 911, and A&W, have a cyber incident response plan. (check the box by for the public safety communication networks that have a cyber incident response plan) <input type="checkbox"/> LMR <input type="checkbox"/> 911 <input type="checkbox"/> Alerts and Warnings Further, the state/territory has contacted its LTE providers to see if they have a cyber incident plan in place. <input type="checkbox"/> Yes <input type="checkbox"/> No
19	NG911 Implementation: NG911 implementation is underway to serve state / territory population.	The state/territory NG911 implementation is in the Legacy or Foundational (Phase I) stages where the ESInet is ready to receive 911 calls from the Originating Service Providers (OSP) via a Legacy Network Gateway	The state/territory NG911 implementation is in the Transitional or Intermediate stages (Phase II) where the ESInet is ready to receive 911 calls in SIP format	The state/territory NG911 implementation is in the End State (Phase III) where the ESInet is ready to receive 911 calls in NG911 format
20	Artificial Intelligence/Machine Learning Incorporation into 911 Call Centers: The state/territory is incorporating Artificial Intelligence/Machine Learning (AI/ML) tools into 911 call centers to assist with analyzing the numerous data streams coming into the center.	The state/territory has not or is not considering incorporating AI/ML tools into 911 call centers within the state/territory	The state/territory is currently considering/researching possible AI/ML tools that could be incorporated into the 911 centers within the state/territory	The state/territory has identified AI/ML tools to utilize in their 911 call centers and has begun implementations

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
21	Data Operability / Interoperability: Ability of agencies within a region to exchange data on demand, and as needed, and as authorized. Examples of systems would be: <ul style="list-style-type: none"> - CAD to CAD - Chat - GIS - Critical Incident Management Tool (i.e. Web EOC) - Patient Care Records (i.e. Transfer of patient from one jurisdiction to the next) 	Agencies are able to share data only by email. Systems are not touching or talking.	Systems are able to touch but with limited capabilities. One way information sharing.	Full system to system integration. Able to fully consume and manipulate data. Two-way information sharing
22	Communications Exercise Objectives: States/Territories have exercised and successfully tested their capabilities against all of FEMA's Operational Communications Core Capabilities standard capability targets	State/Territory has not exercised and tested their capabilities against the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet.	State/Territory has exercised and tested their capabilities against 1 to 2 of the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet. (Check the ones that have been tested in an exercise) <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between federal, tribal, state, and local first responders. <input checked="" type="checkbox"/> Re-establish sufficient communications infrastructure within the affected areas to support ongoing life-sustaining activities, provide basic human needs, and a transition to recovery. <input checked="" type="checkbox"/> Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resilience of key systems. 	State/Territory has successfully exercised and tested their capabilities against all 3 of the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
23	Information and Communications Technology Position Resource Plan: States/Territories have an Information and Communications Technology Position Resource Plan in place and a process for reviewing and refreshing the plan, as needed.	State/Territory is conducting a communications unit needs assessment and/or developing an Information and Communications Technology Position Resource Plan	State/Territory has an Information and Communications Technology Position Resource Plan	State/Territory has an Information and Communications Technology Position Resource Plan and a process for reviewing and refreshing their Information and Communications Technology Position Resource Plan, when needed
24	Incident Communications Resource Coordination Process: Process to develop, maintain, and deploy emergency communications capabilities is implemented and active in state/territory.	<input type="checkbox"/> State/Territory does not have an active program/process to develop, maintain, and deploy emergency communications resources to support incident communications. OR <input type="checkbox"/> State/Territory offers courses in the relevant Information and Communications Technology (ICT) positions and has active enrollment in these courses.	State/territory has an incident communications resource plan, facilitates resource supports an established process for qualification and has an actively engaged resource qualification review board (QRB)	State/territory has an incident communications resource plan, actively engaged QRB, and the state/territory has the ability to deploy/facilitate deployment of incident communications resources
25	Communications Usage Best Practices/Lessons Learned: Thorough after-action reporting, capability and mechanism exists within the state/territory to capture emergency communications best practices/lessons learned activities and share these activities with the appropriate stakeholders and partners.	Does not capture emergency communications best practices/lessons learned activities through after-action reporting	Does capture emergency communications best practices/lessons learned activities through after-action reporting	Does capture emergency communications best practices/lessons learned activities through after-action reporting and proactively shares these activities with stakeholders and partners.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
26	Promoting Priority Telecommunications Services Best Practices: SWIC and/or the emergency communications governing body are actively promoting the use of Priority Telecommunications Services (PTS) within the state/territory.	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 1-2 activities (check all that apply): <input type="checkbox"/> Promoting PTS by distributing relevant information to stakeholders <input type="checkbox"/> Incorporating GETS and WPS into trainings and exercises <input type="checkbox"/> Requesting annual training and education on PTS <input type="checkbox"/> Including PTS programs and products updates on the emergency communications governing body's meeting agenda	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 3 activities (check all that apply): <input checked="" type="checkbox"/> Promoting PTS by distributing relevant information to stakeholders <input checked="" type="checkbox"/> Incorporating GETS and WPS into trainings and exercises <input type="checkbox"/> Requesting annual training and education on PTS <input checked="" type="checkbox"/> Including PTS programs and products updates on the emergency communications governing body's meeting agenda	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 4 activities (check all that apply): <input type="checkbox"/> Promoting PTS by distributing relevant information to stakeholders <input type="checkbox"/> Incorporating GETS and WPS into trainings and exercises <input type="checkbox"/> Requesting annual training and education on PTS <input type="checkbox"/> Including PTS programs and products updates on the emergency communications governing body's meeting agenda
27	Outreach: The SWIC and/or the SWIC's office has outreach mechanisms in place to share information across state.	The SWIC and/or the SWIC office's electronic communication (e.g. SWIC email, newsletter, social media, etc.) is distributed to relevant stakeholders on regular basis	Initial plus the SWIC and/or the SWIC office attends in-person/webinar conference/meeting attendance and is an active participant.	Defined plus the SWIC and/or the SWIC office maintains a current and up-to-date web presence that contains information about emergency communications interoperability, the state PACE plan (if one is in place), SCIP, trainings, interoperable radio programming, etc.
28	Sustainment Management/Planning Cycle: As the technologies' life cycles are getting shorter, states/territories have adapted interoperable component system's sustainment through updated policies and other activities. For example, having an accurate inventory of equipment subject to lifecycle management.	A sustainment assessment plan is in place and includes establishing an end-of-life date for state/territory owned or leased interoperable component systems (e.g. communications infrastructure, equipment, programs, management) that need sustainment funding.	Meets criteria for Initial, plus established a tool that allows the state/territory to track the sustainment plan for the components of the state/territory owned or leased interoperable system.	Meets the criteria for Defined, plus the state/territory has the administration and support needed to maintain a sustainment management system for the components of their owned or leased interoperable systems.
29	Risk Management and Mitigation (PACE Focus): The state/territory has a Primary, Alternative, Contingency, Emergency (PACE) plan in place that has been socialized and exercised.	The state/territory does not have a PACE plan in place	The state/territory is developing a PACE plan	The state/territory has completed a PACE plan within the last two years, and it has been socialized and exercised.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
30	Risk Management and Mitigation (Cybersecurity Focus): The state/territory has a cybersecurity plan that includes emergency communications technologies in place that has been socialized and exercised.	The state/territory does not have a cybersecurity plan that includes emergency communications technologies in place	The state/territory is developing a cybersecurity plan that includes emergency communications technologies	The state/territory has completed a cybersecurity plan that includes emergency communications technologies within the last two years, and it has been socialized and exercised.

APPENDIX B: ACRONYMS

Acronym	Definition
A&W	Alerts and Warnings
AAR	After-Action Report
AI	Artificial Intelligence
ALI	Automatic Location Information
ANI	Automatic Number Identification
APCO	Association of Public-Safety Communications Officials
AUXCOMM/AUXC	Auxiliary Emergency Communications
BDA	Bi-Directional Amplifier
CAD	Computer-Aided Dispatch
CASM	Communication Assets Survey and Mapping
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMMEX	Communications Unit Exercise
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
CSSI	Console Subsystem Interface
DHS	Department of Homeland Security
DPS	Department of Public Safety
EAS	Emergency Alert System
ECC	Emergency Communication Center
EMD	Emergency Medical Dispatch
ESF-2	Emergency Support Function 2
ESInet	Emergency Services Internal Protocol Network
FOG	Field Operations Guide
GETS	Government Emergency Telecommunications System
GIS	Geospatial Information System
HSAC	Homeland Security Advisory Council
ICT	Information and Communications Technology
ICTAP	Interoperable Communications Technical Assistance Program
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
IPAWS	Integrated Public Alerts and Warnings System
ISSI	Inter Subsystem Interface
IT	Information Technology

Acronym	Definition
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MARC	Mid-America Regional Council
MARRS	Metropolitan Area Regional Radio System
MHz	Megahertz
MOSWIN	Missouri' Statewide Interoperability Network
MOU	Memorandum of Understanding
NCSWIC	National Council of Statewide Interoperability Coordinator
NECP	National Emergency Communications Plan
NG911	Next Generation 911
NOAA	National Oceanic and Atmospheric Administration
OCS	Office of Cybersecurity
P25	Project 25
PSAP	Public Safety Answering Point
PTS	Priority Telecommunications Service
PTT	Push-To-Talk
RADO	Radio Operator
SCIP	Statewide Communication Interoperability Plan
SIEC	Statewide Interoperability Executive Committee
SIGB	State Interoperability Governing Board
SLATER	St. Louis Area Trunked Emergency Radio
SOP	Standard Operating Procedure
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TERT	Telecommunications Emergency Response Team
TICP	Tactical Interoperable Communications Plan
TSP	Telecommunications Service Priority
VHF	Very High Frequency
WPS	Wireless Priority Service