OKLAHOMA
STATEWIDE COMMUNICATION INTEROPERABILITY PLAN

January 2025

Developed by the Statewide Interoperability Governance Body with support from the Cybersecurity and Infrastructure Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

Greetings,

As the Statewide Interoperability Coordinator (SWIC) for Oklahoma, I am pleased to present to you the 2025 Oklahoma Statewide Communication Interoperability Plan (SCIP). The SCIP represents the state's continued commitment to improving emergency communications interoperability and supporting the 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 across Oklahoma at the state, county, and local levels collaborated to update the SCIP with actionable and measurable goals and objectives. 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 Oklahoma's level of interoperability maturity by measuring progress against 25 markers. Finally, each goal has an identified champion to ensure completion.

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,

Nikki Dallas
Oklahoma Statewide Interoperability Coordinator
Oklahoma Office of Homeland Security

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 landscape. The SCIP is a guiding document and does not create any authority or direction over any state or local systems or agencies.
- **Vision and Mission** – Articulates Oklahoma's vision and mission for improving emergency and public safety communications interoperability over the next one to three years.
- **Funding** – Describes the funding sources and allocations that support interoperable communications capabilities within Oklahoma along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Governance** – Describes the current governance mechanisms for communications interoperability within Oklahoma as well as successes, challenges, and priorities for improving it.
- **Technology and Cybersecurity** – Outlines public safety technology and operations needed to maintain and enhance interoperability across the emergency communications ecosystem.
- **Implementation Plan** – Describes Oklahoma'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 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.

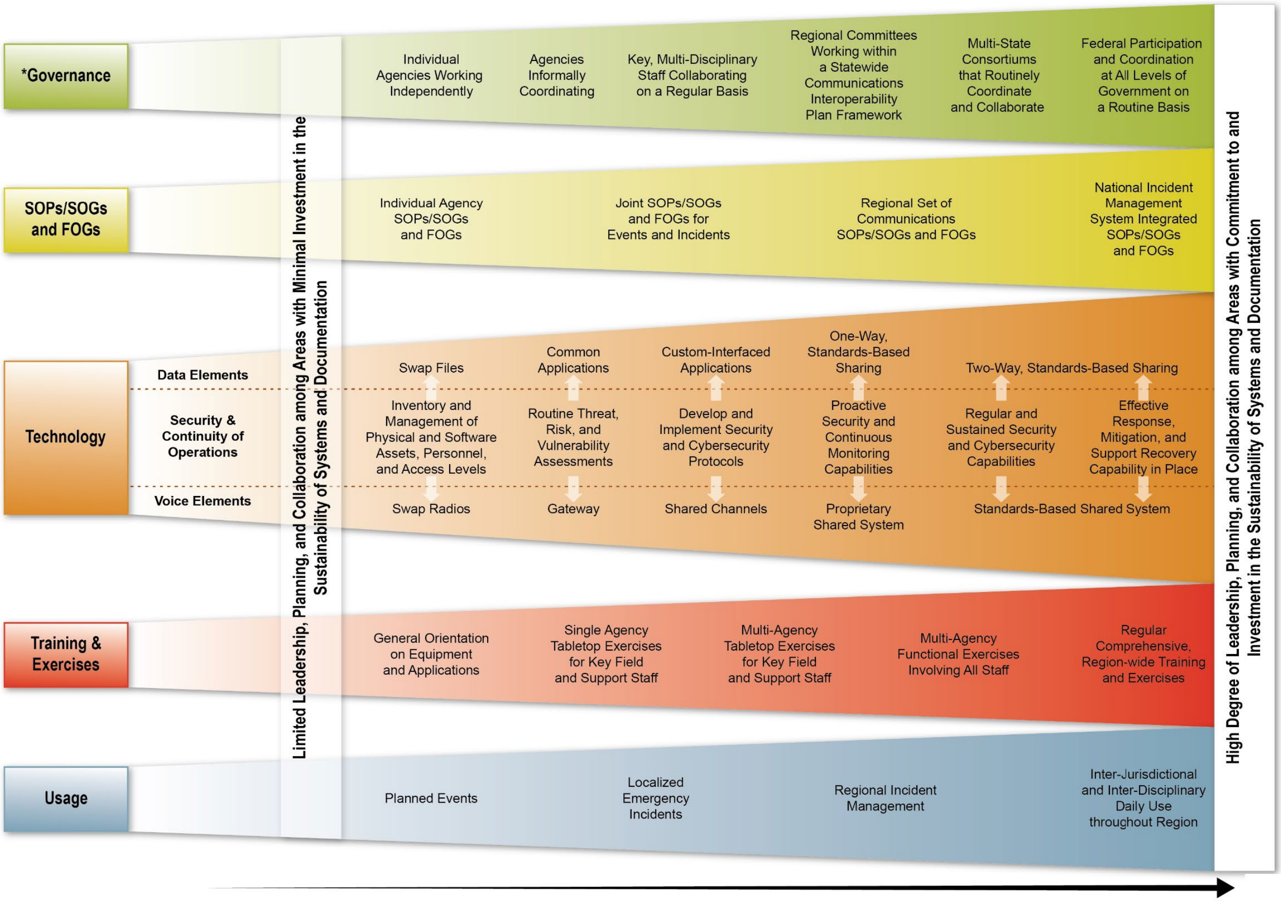
*Governance
Individual Agencies Working Independently
Agencies Informally Coordinating
Key, Multi-Disciplinary Staff Collaborating on a Regular Basis
Regional Committees Working within a Statewide Communications Interoperability Plan Framework
Multi-State Consortiums that Routinely Coordinate and Collaborate
Federal Participation and Coordination at All Levels of Government on a Routine Basis
SOPs/SOGs and FOGs
Individual Agency SOPs/SOGs and FOGs
Joint SOPs/SOGs and FOGs for Events and Incidents
Regional Set of Communications SOPs/SOGs and FOGs
National Incident Management System Integrated SOPs/SOGs and FOGs
Technology
Data Elements
Swap Files
Common Applications
Custom-Interfaced Applications
One-Way, Standards-Based Sharing
Two-Way, Standards-Based Sharing
Security & Continuity of Operations
Inventory and Management of Physical and Software Assets, Personnel, and Access Levels
Routine Threat, Risk, and Vulnerability Assessments
Develop and Implement Security and Cybersecurity Protocols
Proactive Security and Continuous Monitoring Capabilities
Regular and Sustained Security and Cybersecurity Capabilities
Effective Response, Mitigation, and Support Recovery Capability in Place
Voice Elements
Swap Radios
Gateway
Shared Channels
Proprietary Shared System
Standards-Based Shared System
Training & Exercises
General Orientation on Equipment and Applications
Single Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Functional Exercises Involving All Staff
Regular Comprehensive, Region-wide Training and Exercises
Usage
Planned Events
Localized Emergency Incidents
Regional Incident Management
Inter-Jurisdictional and Inter-Disciplinary Daily Use throughout Region
Limited Leadership, Planning, and Collaboration among Areas with Minimal Investment in the Sustainability of Systems and Documentation
High Degree of Leadership, Planning, and Collaboration among Areas with Commitment to and Investment in the Sustainability of Systems and Documentation

Figure 1: Interoperability Continuum

Interoperability and Emergency Communications Overview

Oklahoma Senate Bill 1371 (SB1371) moved the Office of Homeland Security to the Department of Public Safety and requires an updated SCIP annually. SB1371 directs state agencies to comply with provisions of the SCIP. All state agencies are directed to review SCIP requirements prior to the purchase, acquisition, development or enhancement of any public safety communications system. SB1371 further notes that no state agency shall use state funds for such purposes unless that request is consistent with SCIP guidelines. State agencies must also coordinate with the SCIP and the Office of Homeland Security on the applications for, and usage of, public safety radio licenses, as well as channels and frequency allocations.

Interoperability is the ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and types 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, save 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

[2] Interoperability Continuum Brochure

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, communications functions, and levels of government 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) a technology that will enhance the sharing of critical information in real-time using multimedia—such as pictures, video, and text—among citizens, PSAP operators, dispatch, and first responders. While the 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 Oklahoma's vision and mission for improving emergency and public safety communications interoperability:

Vision:

All public safety entities in the state of Oklahoma will possess the knowledge, resources, and technology to effectively communicate during routine and multijurisdictional events as authorized through voice and data, on demand, and in real-time within an interoperability framework.

Mission:

Aligning with federal guidelines, ensure the highest level of public safety interoperable communications across the state of Oklahoma by developing a collaborative framework that supports comprehensive planning, training, and efficient allocation of resources for stakeholders statewide.

FUNDING

The state of Oklahoma is investing approximately $1.3 billion in state and federal funding for broadband infrastructure and accessibility. Oklahoma also received $4,847,500 in Fiscal Year (FY) 2023 from the State Homeland Grant Program (SHSP), part of the Homeland Security Grant Program (HSGP). Local funding for 911 comes from wireless and wireline sources. Wireless funding is collected by the Oklahoma Tax Commission, whereas wireline funds are collected at the local level and are based on local tax rates and fees. Limited state funding is available, and the state-operated Oklahoma Wireless Information Network (OKWIN) needs a new source of funding.

Statewide organizations representing County Commissioners, police chiefs, sheriffs, municipalities, and fire chiefs exert substantial influence into the legislative process. During the SCIP process, participants identified the need to get all these organizations to support a common vision and goal to effectively fund public safety communications in Oklahoma, and that without their collaboration and support, any such effort would be moot.

Funding **challenges** identified during the SCIP process showed the disparity in funding levels between urban and rural agencies.

- Non-urban agencies face funding challenges in the transition to P25 Phase II, and local agencies have difficulty obtaining adequate funding of for LMR.
- OKWIN is a state funded system and primarily serves rural communities, unlike the urban systems that are locally funded.
- There is no statewide funding solution for public emergency communications, and current earmarked funds come from the Department of Public Safety (DPS).

Oklahoma's **desired state for funding** is to have a sustainable, efficient funding strategy that pursues cost-reducing efforts without reducing the quality of public service. This will involve identifying funding requirements for public safety communications. NG911 will have a sustainable funding strategy. Coordination and resource-sharing between agencies will reduce cost through programs such as "upcycling" of equipment and the bulk purchase of technology. This coordination will also increase resiliency and redundancy in PSAPs at less cost.

Funding goals and objectives include the following:

Funding	
Goals	**Objectives**
1. Facilitate the development of an executive level working group representing the Association of County Commissioners of Oklahoma (ACCO), the Police Chiefs' Association of Oklahoma (PCAO), the Oklahoma Sheriff's Association (OSA), the Oklahoma Municipal League (OML), and the Oklahoma Fire Chiefs' Association (OFCA)	1.1 Develop a vision and a needs document to share with executive working group
	1.2 Develop a set of talking points to share with executive working group

GOVERNANCE

In 2009, Oklahoma established the Statewide Interoperability Governing Body (SIGB) under the Oklahoma Office of Homeland Security (OKOHS) by merging two previous governing bodies, the Oklahoma Interoperability Executive Committee (OIEC) and the Governance Working Group (GWG). The SIGB is a formal group of local, county, state, tribal, federal, and authorized non-governmental stakeholders working to improve interoperability.

As part of the SCIP development process, webinars were held with Oklahoma stakeholders, which identified numerous interoperability challenges, emerging issues, threats and risks, and desired states across emergency communications.

The **challenges** identified during the SCIP process highlight a significant need for clear responsibility and authority in the emergency communications space. The SIGB lacks the power to make positive change, and the state-operated OKWIN is not defined in law. This lack of doctrine and authority has hampered coordination, with disparate offerings from key vendors and competition between agencies' individual and currently autonomous radio systems. No single agency is legally or practically capable of bringing all other agencies and regions under the same set of rules and policies.

Furthermore, a significant training and education gap exists across systems, especially when comparing rural vs. urban areas. Rural systems have much smaller budgets and fewer personnel, and expanding to improve both training and education is difficult. As current technicians retire, it has become difficult to hire replacement radio frequency (RF) technicians as people look to other industries for employment.

Emerging issues, such as NG911 and encryption adoption across systems, are well understood by Oklahoma. Its NG911 program has secure funding that the state is confident will endure. The process of adopting LMR encryption standards statewide has also uncovered gaps in encryption education and training.

Additional **governance threats and risks** faced by Oklahoma include new possibilities, such as cyberattacks augmented by machine learning algorithm, as well as ongoing concerns, such as the lack of redundant connections in rural areas and the continuity of operations for communications in general. Commercial vendors do not share all their connections, making it impossible to see how different systems are linked and interdependent, increasing the risk of losing communications if a system goes down.

Oklahoma's governance **desired states** begin with a robust SIGB that works with influential decision-makers at the highest levels of the state legislature, governor's office, state agencies, and county, tribal, and local fire and police departments. This will allow the SIGB to push for a Memorandum of Understanding (MOU) between disparate system-owning agencies, as well as disseminate training and knowledge, such as an Alerts and Warnings guidance document, to all stakeholders. This unified body can also identify and encourage the expansion of training pathways for the next generations of RF technicians and practitioners.

Oklahoma's emergency communications governance map is depicted in Figure 2.

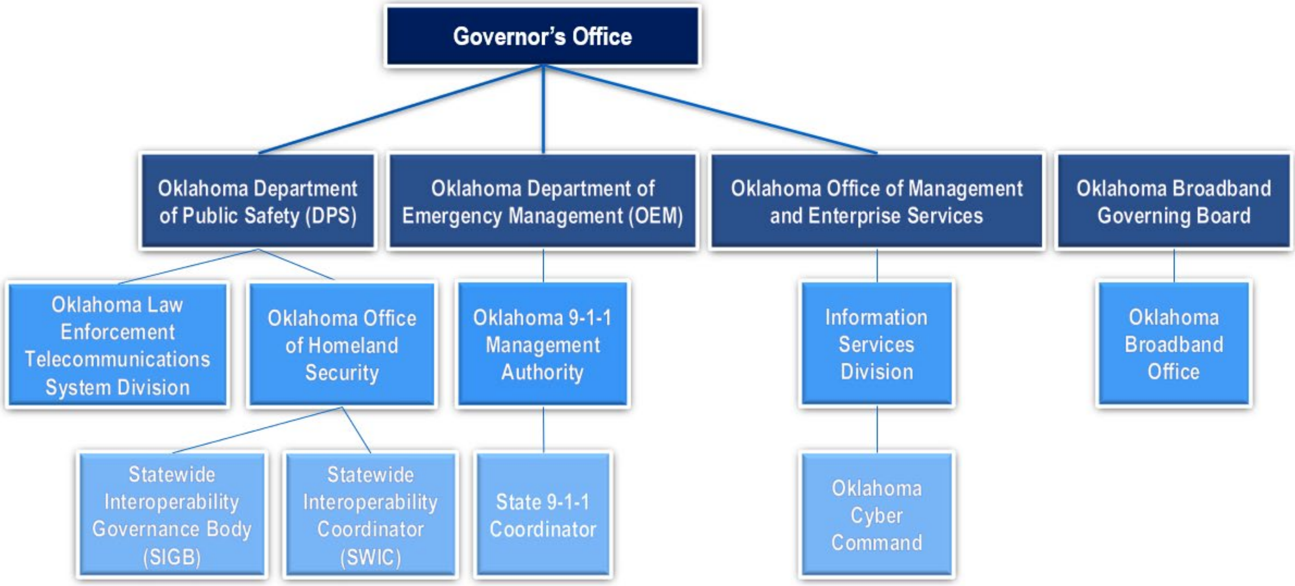
Governor's Office
Oklahoma Department of Public Safety (DPS)
Oklahoma Department of Emergency Management (OEM)
Oklahoma Office of Management and Enterprise Services
Oklahoma Broadband Governing Board
Oklahoma Law Enforcement Telecommunications System Division
Oklahoma Office of Homeland Security
Oklahoma 9-1-1 Management Authority
Information Services Division
Oklahoma Broadband Office
Statewide Interoperability Governance Body (SIGB)
Statewide Interoperability Coordinator (SWIC)
State 9-1-1 Coordinator
Oklahoma Cyber Command

Figure 2: Oklahoma's Emergency Communications Governance Map

Governance goals and objectives include the following:

Governance	
Goals	**Objectives**
2. Enhance Alerts and Warnings guidance for state, tribal, and local entities	2.1 Develop a best practices guide for de-conflicting alerts and warnings messages and message development. Guidance could be placed in OK Field Operations Guide (FOG)
	2.2 Leverage collaboration with education institutions, the Oklahoma School Security Institute, Oklahoma School Security Institute (OSSI), Department of Education, etc. to enhance school safety
	2.3 Develop a working document, including a decision tree and best practices guide, to increase understanding of alerting software and processes
3. Increase coordination between SIGB and potential new or enhanced governance bodies	1.1 Strengthen continuity and collaboration between governance bodies
4. Build a robust SIGB working with true decision makers at the highest levels (state legislature, governor's office, agency decision makers from DPS, fire and police, tribal and local representation, etc.) to enhance integration of disparate radio networks/systems statewide	4.1 Create or identify feasibility of a legislative liaison to assist SIGB
	4.2 Identify other legislative liaisons that can share in the mission
5. Create an actionable MOU and supporting processes between disparate LMR system-owning agencies	5.1 Create working group to develop MOU template
6. Increase public safety communications Education and Outreach	6.1 Create best practices guide from state encryption plan
	6.2 Develop a training guide/best practices to share that covers voice and data
	6.3 Identify and encourage expansion of training pathways for next generations of RF practitioners (see South Dakota for example)
7. Enhance working relationships and partnerships with broadband providers and public safety LMR systems (Primary, Alternate, Contingency, and Emergency [PACE] planning)	7.1 Encourage the expansion of private/public partnerships
	7.2 Pursue federal and state grant opportunities

Governance	
Goals	**Objectives**
8. Establish forward-leaning posture for public safety incident preparedness	8.1 Leverage cybersecurity opportunities across local, state, and federal agencies to prepare for cyber incidents and preparation for statewide system integration
	8.2 Ensure compliance with all state and federal cyber incident reporting requirements (Cyber Incident Reporting for Critical Infrastructure Act [CIRCIA] 2022)
	8.3 Establish continuity of operations planning between PSAPs to ensure seamless operation without service interruption, including Geographic Information System (GIS), voice, data, metadata
	8.4 Engage state associations to support enhanced cybersecurity efforts
	8.5 Increased information sharing on cyber incidents across the state (public and private sector)

TECHNOLOGY AND CYBERSECURITY

LMR

Within Oklahoma, there are five shared LMR networks:

- OKWIN;
- Oklahoma City Radio System;
- Broken Arrow Communications Regional Network (BACRN);
- City of Norman Radio System; and
- Oklahoma Multiple Agency Communications Systems (OMACS).

OKWIN is the largest statewide LMR network, an 800 megahertz (MHz) trunked public safety communications radio system with 43 sites. It provides coverage for 70 percent of Oklahoma's population. Working in concurrence with the OKWIN system are the Oklahoma City Radio System (OCRS) and the BACRN, which provide coverage to the two largest population centers.

Outside of major metropolitan areas, localities rely mainly on stand-alone, but occasionally shared, Very High Frequency (VHF) systems for radio communications.

The LMR **challenges** identified during the SCIP process primarily stem from a lack of coordination and governance structure. The state has struggled to establish a strong governance body, and the resulting lack of interoperability requirements between manufacturers has hindered the establishment of an Inter-RF Subsystem Interface (ISSI) between OKWIN and OK City, even though the physical capability exists. Finally, LMR education in rural communities is often lacking, especially across fire departments and law enforcement.

The LMR **emerging issues and risks** faced by Oklahoma pertain to both reliable system backups and meeting long term staffing requirements. The state has begun to look at using an Emergency Services IP Network (ESInet) as a backup for LMR or Broadband. It has also become increasingly difficult to find and keep trained and knowledgeable RF personnel.

Oklahoma's **desired state** for LMR focuses on interoperability between systems and long-term system sustainment. This includes a statewide LMR strategic plan and integration requirements for LMR and Long-Term Evolution (LTE) gateways. This will ideally achieve an ISSI with auto-roaming functionality between OKWIN and OK City. Oklahoma also wishes to expand their Radio 100 and Radio 101 basic training courses, especially in rural communities. Enhanced collaboration with higher education and military institutions was seen as a way to identify and promote pathways to RF careers.

911

The Oklahoma 911 Management Authority oversees the development and operation of emergency 911 systems within the state of Oklahoma. This includes 126 local and county primary PSAPs and 8 secondary PSAPs. Multiple standalone emergency communications centers (ECCs) handle emergency calls for local fire, police, state parks, lakes and waterways, military bases, and certain restricted tribal properties.

NG911 has experienced strong support within Oklahoma, with recently increased funding. It is expected that this support will continue without issue.

The **challenges** faced by Oklahoma's 911 systems are similar to those in LMR. A significant training and education gap exists across systems, especially when comparing urban vs rural communities. It has been difficult to get all areas of the state up to 911/Enhanced 911 (E911) functionality. This has led to an **emerging issue,** where some areas have sought their own NG911 platform, independent of the state. A lack of continuity of operations planning (COOP) creates a **risk** of communication disruption between PSAPs.

Oklahoma's **desired states** for 911 primarily relate to communication and coordination between PSAPs. NG911 should ultimately allow for interoperability between PSAPs. PSAPs and ECCs will use available technology and funding to enhance their continuity of operations planning and support the sharing of resources (facilities, technology, cache radios, etc.) to increase the resiliency and redundancy of PSAPs. This will allow for the seamless provision of 911 services without interruption, including GIS, voice, data, and metadata (data that describes other data, such as information identifying the origin and time of texts but not the message contained within it). PSAPs and ECCs will also make use of integrated and emerging technologies to increase their efficiency and efficacy. Furthermore, the areas of the state that have deployed E911 would increase their cohesion and coordination.

Broadband

In January 2021, FirstNet announced that Oklahoma's Public Safety Broadband Network (PSBN) build-out was ahead of schedule and includes new, purpose-built FirstNet cell sites and other network enhancements. As of that announcement, 12 counties across Oklahoma designated cell sites for the PSBN. Oklahoma's PSBN cell sites use Band 14 spectrum, as well as AT&T commercial spectrum. As of August 2024, Band 14 spectrum has been deployed on nearly 1,300 sites across the state.

Oklahoma has strong support for public safety across the state, with funding readily available for fixing the present problems. However, there is no consensus on a specific solution.

Oklahoma faces **challenges** from the commercial broadband vendors who sell their products primarily as a replacement to, and not a supplement for, LMR. Broadband devices operate on 3GPP standards rather than the LMR's P25 standards, further reducing the ability of these devices and systems to interoperate. Broadband sites also cover a much smaller area compared to radio, requiring many more sites to cover the same amount of territory.

Oklahoma also faces the **risk** that cell networks are not hardened against attack or disruption to the same degree as public safety radio systems. In an emergency, broadband networks are much more easily overwhelmed, congested, or taken down entirely.

The **desired state** for Oklahoma's public safety broadband relies on improving relationships between broadband providers and public safety LMR systems. The expansion of public/private partnerships will improve network and device interoperability. Additionally, Oklahoma will more aggressively pursue federal and state grant opportunities to expand the broadband accessibility.

Alerts and Warnings

Most Oklahomans rely on the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS), through which federal, state, local, and tribal officials send alerts. There are 26 IPAWS Alerting Authorities in the state. The Oklahoma Weather Alert Remote Notification (OK-WARN) provides notification of weather hazards and emergencies to deaf and hard-of-hearing Oklahomans via pager, email, or cell phone. Efforts are ongoing to make alerts and warnings both more efficient and effective.

The SCIP process determined that the greatest alerts and warning **challenge** for Oklahoma is the limited coordination among stakeholders. Without strong coordination, there is a **risk** of too many messages and alerts being shared, leading to message fatigue. An important **emerging issue** is school safety, with the rise in attacks on school properties.

Oklahoma's **desired state** for its Alerts and Warnings systems focuses on de-conflicting messaging and avoiding message fatigue. A best practices guide should be developed and shared among stakeholders to increase the clarity, accuracy, and effectiveness of emergency messaging. Oklahoma also seeks to improve the understanding of alerting software and processes that are currently in-use. Finally, Oklahoma hopes to leverage collaboration with educational institutions, the OSSI, the Department of Education, and others to enhance school safety.

Technology and Cybersecurity for Public Safety

In response to increasing cyber threats to Oklahoma, the Oklahoma Information Sharing and Analysis Center (OK-ISAC) was established in August 2020 as a multiagency effort led by the Office of Management and Enterprise Services (OMES). OK-ISAC focuses on mitigating cybersecurity risks across the state, providing real-time monitoring, vulnerability identification, incident response and threat intelligence to its members and partners. OK-ISAC currently includes eight members from emergency services and 14 members from communications.

During the SCIP process, the stakeholders determined that the most significant **challenge** for public safety technology and cybersecurity is funding. Budget constraints prevent smaller agencies and entities from upgrading and maintining their systems. This, in turn, can create **risks** from using legacy, outdated systems. Lack of training and knowledge among technology users is also a signficant risk. Social engineering is an **emerging issue** that clashes with emergency response, as malicious individuals may use emergency services to harrass targets or disrupt events.

Oklahoma's **desired state** for cybersecurity focuses on improved information sharing, resource awareness, and cyber training. The state will seek to identify and implement all available federal resources to protect public safety communications. It will also seek to promote increased information sharing on cyber incidents across the state's public and private sectors, as well as to ensure compliance with all state and federal cyber incident reporting requirements. This will coincide with further leveraging opportunities at the state, local, and federal level to prepare for cyber incidents and statewide system integration. Finally, Oklahoma will look to establish basic cyber hygiene among public safety practicioners and increase overall security education awareness training.

Technology and cybersecurity goals and objectives include the following:

Technology and Cybersecurity	
Goals	**Objectives**
9. Enhance the role of National Incident Management System (NIMS) Incident Command System (ICS) within incident communications in the field	9.1 The Communications Unit Plan (COMU) will serve as the authority for communications positions for state NIMS ICS unit positions into the "state incident management team" (new title pending)
	9.2 Enhance outreach and education of NIMS ICS unit capabilities
10. Design, maintain, and protect a cybersecure ecosystem to support public safety communications	10.1 Establishment of basic cyber hygiene practices among public safety practitioners
	10.2 Engage state associations to support enhanced cybersecurity efforts.
	10.3 Identify and implement federal cybersecurity resources to protect public safety communications in Oklahoma
11. Leverage technology to enhance continuity of operations planning and encourage sharing of resources to increase the resiliency and redundancy of PSAPs in Oklahoma	11.1 Utilize integrated technology and emerging technologies to increase efficiency and efficacy
	11.2 Identify the potential to share facilities, technology, and equipment between PSAPs
	11.3 Educate agency leadership and elected officials to leverage technology to enhance cybersecurity for public safety agencies.
12. Increase cohesion between the multiple islands of enhanced 911 deployment in the state and increased standardization of information and deployment	12.1 Enhance interoperability between PSAPs, including backups and fail over
	12.2 Support the NG911 master plan to provide effective and consistent service across the state
	12.3 Encourage consolidation of PSAPs in order to effect operational efficiencies

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. The Cybersecurity and Infrastructure Security Agency's (CISA) Interoperable Communications Technical Assistance Program (ICTAP) has a catalog[3] of technical assistance (TA) available to assist with the implementation of goals within the SCIP. TA requests are to be coordinated through the SWIC.

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

Goals	Objectives	Owners	Completion Dates
1. Facilitate the development of an executive level working group representing the ACCO, PCAO, OSA, OML, and OFCA	1.1 Establishment of basic cyber hygiene practices among public safety practitioners Develop a vision and a needs document to share with executive working group	SWIC State 911 Coordinator's Office SIGB	Q4 2024/ASAP
	1.2 Develop a set of talking points to share with executive working group	State 911 Coordinator's Office SIGB	Q4 2024/ASAP
2. Enhance Alerts and Warnings guidance for state, tribal, and local entities.	2.1 Develop a best practices guide for de-conflicting and message development. Guidance could be placed in OK FOG	SWIC	Q3 2025
	2.2 Leverage collaboration with education institutions, OSSI, Department of Education, etc. to enhance school safety	SIGB/SWIC	Q3 2025
	2.3 Develop a working document, including a decision tree and best practices guide, to increase understanding of alerting software and processes in use	SWIC/OEM/ DPS	Q2 2026
3. Increase coordination between SIGB and potential new governance bodies	3.1 Strengthen continuity and collaboration between governance bodies	SIGB/SWIC	Ongoing
4. A robust SIGB working with true decision makers	4.1 Create or identify feasibility of a legislative liaison to assist SIGB	SWIC/SIGB	February 2025

[3] Emergency Communications Technical Assistance Planning Guide

Goals	Objectives	Owners	Completion Dates
at the highest levels (state legislature, governor's office, agency decision makers from DPS, fire and police, tribal and local representation, etc.) to enhance integration of disparate radio networks/systems statewide	4.2 Identify other legislative liaisons that can share in the mission	SWIC 911 Coordinator	Q1 2025
5. Create a strong MOU program between disparate system-owning agencies	5.1 Create working group to develop MOU template	SIGB/SWIC	Q2 2025
6. Increase public safety communications Education and Outreach	6.1 Create best practices guide from state encryption plan	SIGB	Q3 2025
	6.2 Develop a training guide/best practices to share that covers voice and data	SWIC 911 Coordinator's Office	Q1 2026
	6.3 Identify and encourage expansion of training pathways for next generations of RF practitioners (see South Dakota for example)	OKC SWIC/Deputy SWIC AUXCOMM	Ongoing
7. Enhanced working relationships and partnerships with broadband providers and public safety LMR systems (PACE planning)	7.1 Encourage the expansion of private/public partnerships	SIGB	Ongoing
	7.2 Pursue federal and state grant opportunities	OKC SWIC/SIGB DPS System Owners	Ongoing
8. Establish forward-leaning posture for public safety incident preparedness	8.1 Leverage cybersecurity opportunities at the local, state, and federal level to prepare for cyber incidents and preparation for statewide system integration	OK-ISAC SIGB	Q3 2025

Goals	Objectives	Owners	Completion Dates
	8.2 Ensure compliance with all state and federal cyber incident reporting requirements (CIRCIA 2022)	CISA OK-ISAC	Ongoing
	8.3 Continuity of operations between PSAPs to ensure seamless operation without service interruption, including GIS, voice, data, metadata	911 State Coordinator's Office	Ongoing
	8.4 Engage state associations to support enhanced cybersecurity efforts	OK-ISAC SIGB Cybersecurity Working Group	Ongoing
	8.5 Increased information sharing on cyber incidents across the state (public and private sector)	OK-ISAC	Ongoing
9. Enhance the role of NIMS ICS within incident communications in the field	9.1 The Communications Unit Plan will serve as the authority for communications positions for state NIMS ICS unit positions into the "state incident management team" (new title pending)	SWIC/Deputy SWIC COMU	Ongoing
	9.2 Enhance outreach and education of NIMS ICS unit capabilities	SWIC/Deputy SWIC COMU	Ongoing
10 Design, maintain, and protect a cybersecure ecosystem to support public safety communications	10.1 Establishment of basic cyber hygiene practices among public safety practitioners	Cyber working group OK-ISAC	Q3 2025
	10.2 Identify and implement federal cybersecurity resources to protect public safety communications in Oklahoma	OK-ISAC CISA Cybersecurity Working Group	Ongoing
11 Leverage technology to enhance continuity of operations planning and encourage sharing of resources to increase the resiliency and redundancy of PSAPs in Oklahoma	11.2 Utilize integrated technology and emerging technologies to increase efficiency and efficacy	State 911 Coordinator's Office	Ongoing
	11.2 Identify the potential to share facilities, technology, and equipment	State 911 Coordinator's Office	Ongoing

Goals	Objectives	Owners	Completion Dates
	11.3 Educate agency leadership and elected officials to leverage technology to increase operational efficiency	State 911 Coordinator's Office	Ongoing
12. Increase cohesion between the multiple islands of enhanced 911 deployment in the state and increased standardization of information and deployment	12.1 Enhance interoperability between PSAPs, including backups and fail over	State 911 Coordinator's Office	Q2/3 2026
	12.2 Support the NG911 master plan to provide effective and consistent service across the state	State 911 Coordinator's Office SIGB	Ongoing
	12.3 Encourage consolidation of PSAPs in order to effect operational efficiencies	State 911 Coordinator's Office SIGB	Ongoing

APPENDIX A: STATE MARKERS

In 2019, CISA supported states and territories in establishing an initial picture of interoperability nationwide by measuring progress against 25 markers. These markers describe a state or territory's level of interoperability maturity. Below is Oklahoma's assessment of their progress against the markers as of 12/31//24.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
1	**State-level governing body established (e.g., SIEC, SIGB).** Governance framework is in place to sustain all emergency communications	Governing body does not exist, or exists and role has not been formalized by legislative or executive actions	Governing body role established through an executive order	Governing body role established through a state law
2	**SIGB/SIEC participation.** Statewide governance body is comprised of members who represent all components of the emergency communications ecosystem.	Initial (1-2) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications	Optimized (5) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 911 ☒ Alerts, Warnings and Notifications
3	**SWIC established.** Full-time SWIC is in place to promote broad and sustained participation in emergency communications.	SWIC does not exist	Full-time SWIC with collateral duties	Full-time SWIC established through executive order or state law
4	**SWIC Duty Percentage.** SWIC spends 100% of time on SWIC-focused job duties	SWIC spends <50% of time on SWIC-focused job duties	SWIC spends 50-90% of time on SWIC-focused job duties	SWIC spends >90% of time on SWIC-focused job duties
5	**SCIP refresh.** SCIP is a living document that continues to be executed in a timely manner. Updated SCIPs are reviewed and approved by SIGB/SIEC.	No SCIP OR SCIP older than 3 years	SCIP updated within last 2 years	SCIP updated in last 2 years and progress made on >50% of goals
6	**SCIP strategic goal percentage.** SCIP goals are primarily strategic to improve long term emergency communications ecosystem (LMR, LTE, 911, A&W) and future technology transitions (5G, IoT, UAS, etc.). (Strategic and non-strategic goals are completely different; strategy -- path from here to the destination; it is unlike tactics which you can "touch"; cannot "touch" strategy)	<50% are strategic goals in SCIP	50%-90% are strategic goals in SCIP	>90% are strategic goals in SCIP

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
7	**Integrated emergency communication grant coordination.** Designed to ensure state/territory is tracking and optimizing grant proposals, and there is strategic visibility 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 SIGB provides guidance to agencies and localities for emergency communications grant funding but does not review proposals or make recommendations	SWIC and/or SIGB provides guidance to agencies and localities for emergency communications grant funding and reviews grant proposals for alignment with the SCIP. SWIC and/or SIGB provides recommendations to the SAA
8	**Communications Unit process.** Communications Unit process present in state/territory to facilitate emergency communications capabilities. Check the boxes of which Communications positions are currently covered within your process: ☒ COML ☒ COMT ☒ ITSL ☒ RADO ☒ INCM ☒ INTD ☒ AUXCOM ☐ TERT	No Communications Unit process at present	Communications Unit process planned or designed (but not implemented)	Communications Unit process implemented and active
9	**Interagency communication.** Established and applied interagency communications policies, procedures and guidelines.	Some interoperable communications SOPs/SOGs exist within the area and steps have been taken to institute these interoperability procedures among some agencies	Interoperable communications SOPs/SOGs are formalized and in use by agencies within the area. Despite minor issues, SOPs/SOGs are successfully used during responses and/or exercises	Interoperable communications SOPs/SOGs within the area are formalized and regularly reviewed. Additionally, NIMS procedures are well established among agencies and disciplines. All needed procedures are effectively utilized during responses and/or exercises.
10	**TICP (or equivalent) developed.** Tactical Interoperable Communications Plans (TICPs) established and periodically updated to include all public safety communications systems available	Regional or statewide TICP in place	Statewide or Regional TICP(s) updated within past 2-5 years	Statewide or Regional TICP(s) updated within past 2 years
11	**FOGs developed.** FOGs established for a state or territory and periodically updated to include all public safety communications systems available	Regional or statewide FOG in place	Statewide or Regional FOG(s) updated within past 2-5 years	Statewide or Regional FOG(s) updated within past 2 years

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
12	**Alerts & Warnings.** State or Territory has Implemented an effective A&W program to include Policy, Procedures and Protocol measured through the following characteristics: (1) Effective documentation process to inform and control message origination and distribution (2) Coordination of alerting plans and procedures with neighboring jurisdictions (3) Operators and alert originators receive periodic training (4) Message origination, distribution, and correction procedures in place	<49% of originating authorities have all four of the A&W characteristics	50%-74% of originating authorities have all four of the A&W characteristics	>75% of originating authorities have all four of the A&W characteristics
13	**Radio programming.** Radios programmed for National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state/territory.	<49% of radios are programed for interoperability and consistency	50%-74% of radios are programed for interoperability and consistency	>75% of radios are programed for interoperability and consistency
14	**Cybersecurity Assessment Awareness.** Cybersecurity assessment awareness. (Public safety communications networks are defined as covering: LMR, LTE, 911, and A&W)	Public safety communications network owners are aware of cybersecurity assessment availability and value (check yes or no for each option) ☐ LMR ☐ LTE ☐ 911/CAD ☐ A&W	Initial plus, conducted assessment, conducted risk assessment. (Check yes or no for each option) ☒ LMR ☒ LTE ☒ 911/CAD ☒ A&W	Defined plus, Availability of Cyber Incident Response Plan (check yes or no for each option) ☐ LMR ☐ LTE ☐ 911/CAD ☐ A&W
15	**NG911 implementation.** NG911 implementation underway to serve state/territory population.	Working to establish NG911 governance through state/territorial plan. • Developing GIS to be able to support NG911 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • Planning to or have updated PSAP equipment to handle basic NG911 service offerings.	>75% of PSAPs and Population Served have: • NG911 governance established through state/territorial plan. • GIS developed and able to support NG911 call routing. • Planning or implementing ESInet and NGCS. • PSAP equipment updated to handle basic NG911 service offerings.	> 90% of PSAPs and Population Served have: • NG911 governance established through state/territorial plan. • GIS developed and supporting NG911 call routing. • Operational Emergency Services IP Network (ESInet)/NGCS. • PSAP equipment updated and handling basic NG911 service offerings.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
16	**Data operability/interoperability.** Ability of agencies within a region to exchange data on demand, and needed, and as authorized. Examples of systems would be: CAD to CAD, Chat, GIS, Critical Incident Management Tool, Web EOC	Agencies can share data only by email. Systems are not touching or talking.	Systems can touch but with limited capabilities. One-way information sharing.	Full system to system integration. Able to fully consume and manipulate data.
17	**Future Technology/Organizational Learning.** SIEC/SIGB is tracking, evaluating, implementing future technology (checklist)	☒ 5G ☒ Acoustic Signaling ☒ Autonomous Vehicles ☒ Body Cameras ☒ ESInets ☒ GIS ☒ Geolocation	☒ HetNets/Mesh Networks ☒ LMR to LTE Integration ☒ MCPTT Apps ☐ Machine Learning/AI ☒ Public Alerting Software ☒ Sensors ☒ Situational Awareness Apps	☒ Smart Cities ☒ The Next Narrowbanding ☒ UAS (Drones) ☒ UAV (Smart Vehicle) ☒ Wearables ☒ IoT (Cameras)
18	**Communications Exercise objectives.** Specific emergency communications objectives are incorporated into applicable exercises Federal/state/territory-wide	Regular engagement with State Training and Exercise coordinators	Promote addition of emergency communications objectives in state/county/regional level exercises (target Emergency Management community). Including providing tools, templates, etc.	Initial and defined plus mechanism in place to incorporate and measure communications objectives into state/county/regional level exercises
19	**Trained Communications Unit responders.** Communications Unit personnel are listed in a tracking database (e.g., NQS One Responder, CASM, etc.) and available for assignment/response.	<49% of public safety agencies within a state/territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response	50%-74% of public safety agencies within a state/territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response	>75% of public safety agencies within a state/territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response
20	**Communications Usage Best Practices/Lessons Learned.** Capability exists within jurisdiction to share best practices/lessons learned (positive and/or negative) across all lanes of the Interoperability Continuum related to all components of the emergency communications ecosystem	Best practices/lessons learned intake mechanism established. Create Communications AAR template to collect best practices	Initial plus review mechanism established	Defined plus distribution mechanism established
21	**Wireless Priority Service (WPS) subscription.** WPS penetration across state/territory compared to maximum potential	<9% subscription rate of potentially eligible participants who signed up WPS across a state/territory	10%-49% subscription rate of potentially eligible participants who signed up for WPS a state/territory	>50% subscription rate of potentially eligible participants who signed up for WPS across a state/territory
22	**Outreach.** Outreach mechanisms in place to share information across state	SWIC electronic communication (e.g., SWIC email, newsletter, social media, etc.) distributed to relevant stakeholders on regular basis	Initial plus web presence containing information about emergency communications interoperability, SCIP, trainings, etc.	Defined plus in-person/webinar conference/meeting attendance strategy and resources to execute

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
23	**Sustainment assessment.** Identify interoperable component system sustainment needs;(e.g., communications infrastructure, equipment, programs, management) that need sustainment funding. (Component systems are emergency communications elements that are necessary to enable communications, whether owned or leased - state systems only)	<49% of component systems assessed to identify sustainment needs	50%-74% of component systems assessed to identify sustainment needs	>75% of component systems assessed to identify sustainment needs
24	**Risk identification.** Identify risks for emergency communications components. (Component systems are emergency communications elements that are necessary to enable communications, whether owned or leased. Risk Identification and planning is in line with having a communications COOP Plan)	<49% of component systems have risks assessed through a standard template for all technology components	>50%-74% of component systems have risks assessed through a standard template for all technology components	>75% of component systems have risks assessed through a standard template for all technology components
25	**Cross Border/Interstate (State to State) Emergency Communications.** Established capabilities to enable emergency communications across all components of the ecosystem.	Initial: Little to no established: ☐ Governance ☐ SOPs/MOUs ☐ Technology ☐ Training/Exercises ☐ Usage	Defined: Documented/established across some lanes of the Continuum: ☐ Governance ☐ SOPs/MOUs ☐ Technology ☐ Training/Exercises ☐ Usage	Optimized: Documented/established across all lanes of the Continuum: ☒ Governance ☒ SOPs/MOUs ☒ Technology ☒ Training/Exercises ☒ Usage

APPENDIX B: ACRONYMS

Acronym	Definition
A&W	Alerts and Warnings
AAR	After-Action Report
AUXCOMM/AUXC	Auxiliary Emergency Communications
BACRN	Broken Arrow Communications Regional Network
CASM	Communication Assets Survey and Mapping
CIRCIA 2022	Cyber Incident Reporting for Critical Infrastructure Act 2022
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
DPS	Department of Public Safety
ESInet	Emergency Services Internal Protocol Network
FOG	Field Operations Guide
GIS	Geospatial Information System
GWG	Governance Working Group
HSGP	Homeland Security Grant Program
ICTAP	Interoperable Communications Technical Assistance Program
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
MHz	Megahertz
MOU	Memorandum of Understanding
NECP	National Emergency Communications Plan
NG911	Next Generation 911
OCRS	Oklahoma City Radio System
OIEC	Oklahoma Interoperability Executive Committee
OK-ISAC	Oklahoma Information Sharing and Analysis Center
OKWIN	Oklahoma Wireless Information Network
OMACS	Oklahoma Multiple Agency Communications Systems
OMES	Office of Management and Enterprise
PSAP	Public Safety Answering Point
PSBN	Public Safety Broadband Network
Radio Frequency	RF

Acronym	Definition
RADO	Radio Operator
SCIP	Statewide Communication Interoperability Plan
SHSP	State Homeland Grant Program
SIGB	Statewide Interoperability Governance Board
SOP	Standard Operating Procedure
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TERT	Telecommunications Emergency Response Team
TICP	Tactical Interoperable Communications Plan
WPS	Wireless Priority Service