



OKLAHOMA STATEWIDE COMMUNICATION INTEROPERABILITY PLAN



September 2021

Developed 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..... 5

 Land Mobile Radio 5

 Public Safety Broadband 5

 9-1-1/Next Generation 9-1-1 6

 Alerts and Warnings..... 6

 Cybersecurity for Public Safety Technology..... 6

Funding..... 7

Implementation Plan 8

Appendix A: State Markers 10

Appendix B: Acronyms 16

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

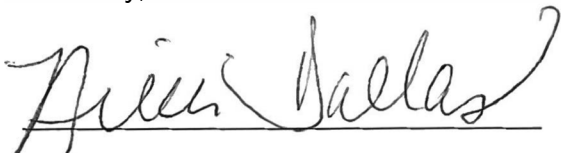
Greetings,

As the Statewide Interoperability Coordinator (SWIC) for Oklahoma, I am pleased to present to you the 2021 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 grant guidelines.

Representatives from across the State of Oklahoma 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 new technologies and navigating the ever-changing emergency communications landscape. They also incorporate the state interoperability markers which describe Oklahoma's level of interoperability maturity by measuring progress against 25 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,

A handwritten signature in cursive script that reads "Nikki Dallas". The signature is written in black ink and is positioned above a horizontal line.

Nikki Dallas
Oklahoma Statewide Interoperability Coordinator
Oklahoma Department of Emergency Management and 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.
- **Governance** – Describes the current governance mechanisms for communications interoperability within Oklahoma, 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 Oklahoma along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **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 inter-related components and functions, including communications for incident response operations, notifications and 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.

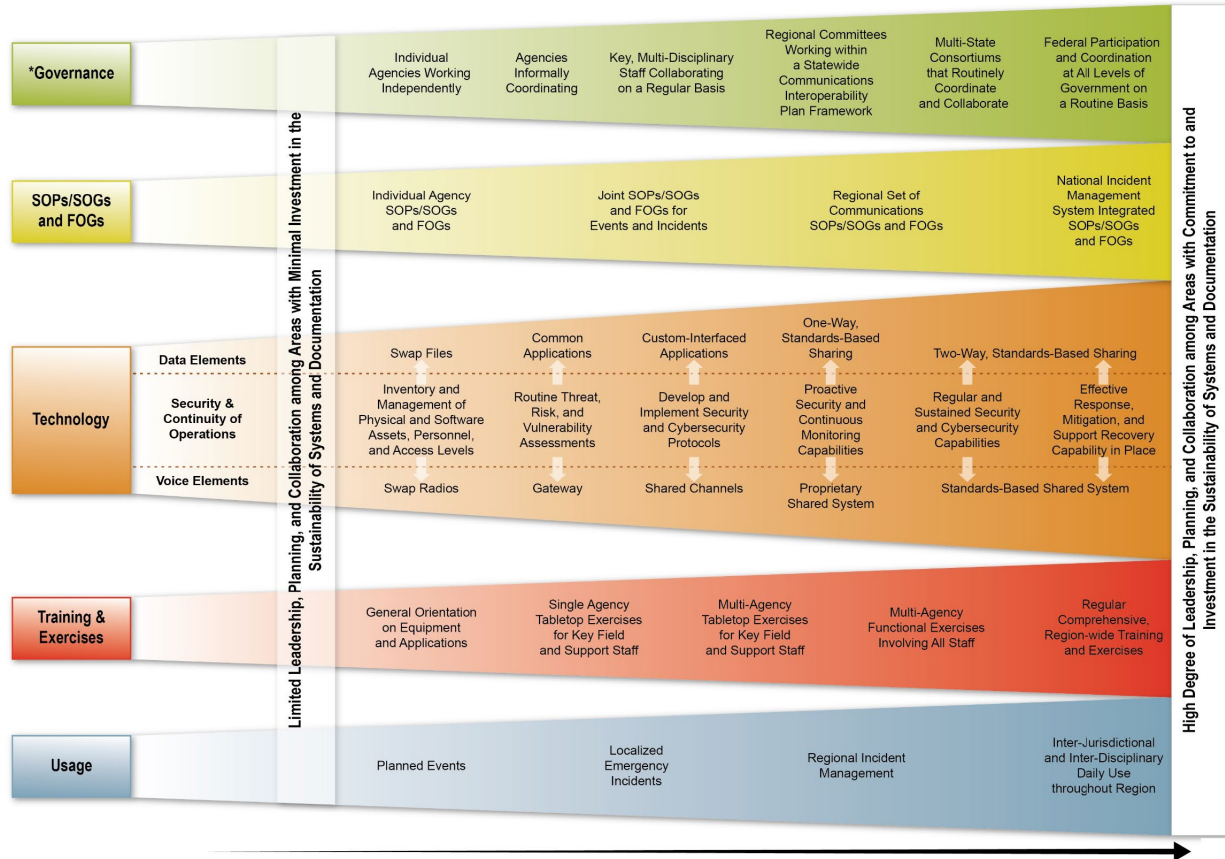


Figure 1: Interoperability Continuum

Interoperability and Emergency Communications Overview

Traditional voice capabilities, such as land mobile radio (LMR) and landline 9-1-1 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. New 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.

² [Interoperability Continuum Brochure](#)

An example of this evolution is the transition of public-safety answering points (PSAPs) to Next Generation 9-1-1 (NG9-1-1) technology that will enhance sharing of critical information in real-time using multimedia – such as pictures, video, and text – among citizens, PSAP operators, dispatch, and first responders. While potential benefits of NG9-1-1 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.

Mission:

In accordance with federal guidelines, ensure the highest level of public safety communications throughout the State of Oklahoma by developing an organizational structure that supports proper planning and training, so resources are available to responders at all levels.

GOVERNANCE

In 2020, Oklahoma Governor Kevin Stitt signed an executive order to place the Oklahoma Office of Homeland Security within the Oklahoma Department of Emergency Management, creating the Oklahoma Department of Emergency Management and Homeland Security (ODEMHS). The ODEMHS office is charged with preparing for, responding to, recovering from, and mitigating against disasters and emergencies. The department maintains the State Emergency Operations Center (EOC), which serves as a command center for reporting emergencies and coordinating state response activities. The ODEMHS delivers service to Oklahoma cities, towns, counties, tribes, and other public and private sector entities through the network of more than 300 local emergency managers. Both the SWIC and Deputy SWIC, as well as the Statewide Interoperable Governance Body (SIGB), are supported by ODEMHS.

The SIGB is a formal group of local, county, state, tribal, federal, and authorized non-governmental stakeholders working to improve interoperability. The SIGB includes various working groups, including the new encryption working group. The encryption working group is focused on finalizing and disseminating the state encryption plan.

The SWIC's office has prioritized information sharing across the Oklahoma public safety community by disseminating an interoperable communications newsletter to more than 500 stakeholders twice a year.

In the future, Oklahoma looks to enhance its interoperability governance documents, including the creation of an Alerts and Warnings guidance document and strengthening regional Tactical Interoperability Communications Plans (TICPs). The ODEMHS recently released an updated version of Oklahoma's Electronic Field Operations Guide (eFOG).

The following table outlines goals and objectives related to Governance:

Governance	
Goal	Objectives
1. Create an Alerts and Warnings guidance document for local government entities	1.1 Request Technical Assistance (TA) for support
	1.2 Encourage the update of the state Emergency Alert System (EAS) plan
	1.3 Weather service capability to issue evacuation orders
2. Increase coordination between the SIGB and new governance bodies	2.1 Enhance continuity and collaboration between governance bodies
3. Strengthen regional TICPs	3.1 Request CISA TA support
4. Create a statewide Project 25 (P25) ID plan and strong Memorandum of Understanding (MOU) program	4.1 Create P25 ID/talkgroup plan working group to include representatives from each LMR system
5. Finalize and disseminate state encryption plan	5.1 Coordinate with encryption working group

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

Agencies in Oklahoma operate five shared LMR networks: the Broken Arrow Communications Regional Network, the Oklahoma City Radio System, the Oklahoma Wireless Information Network (OKWIN), City of Norman Radio System, and the Oklahoma Multiple Agency Communications System (OMACS). These networks are owned and maintained by multiple partner cities and agencies and have all moved to P25. The OKWIN is a 43 site, 800 megahertz (MHz) trunked public safety communications radio system and is the largest statewide LMR network, providing coverage to 70 percent of the State's population. The State completed its transition from P25 Phase I to P25 Phase II in 2020.

Oklahoma is focused on increasing LMR coverage across the state and creating interoperability between the State's multiple LMR systems through the creation of a statewide LMR strategic plan.

Public Safety Broadband

Oklahoma opted into FirstNet in 2017. Stakeholders have identified the need to improve resiliency to FirstNet towers and to integrate the multiple cellular vendors providing public safety broadband support.

9-1-1/Next Generation 9-1-1

The Oklahoma 9-1-1 Management Authority works with the ODEMHS to improve 9-1-1 in the state. The Authority is developing a statewide NG9-1-1 plan to guide the state to deployment. An NG9-1-1 statewide Geographic Information System (GIS) repository has been created and local GIS professionals are being trained on how to meet state GIS data standards and upload their data into the state repository.

The 9-1-1 Association of Central Oklahoma Governments (9-1-1 ACOG) is an intergovernmental entity formed to implement, administer, and coordinate the operation of the regional Enhanced 9-1-1 (E9-1-1) emergency communication service in Central Oklahoma, and provides outreach to 21 PSAPs. Oklahoma looks to create more cohesion and standardized information sharing between the multiple islands of E9-1-1 deployment across the State.

To enhance efficiency, Oklahoma plans to review the current number of PSAPs across the state. The State is also looking to review backup and failover between PSAPs to increase interoperability.

Alerts and Warnings

Oklahoma utilizes the Integrated Public Alert and Warning System (IPAWS). Stakeholders identified the need for a statewide Alerts and Warnings guidance document, as well as an update to the state Emergency Alert System (EAS) plan.

Cybersecurity for Public Safety Technology

The Oklahoma Office of Management and Enterprise Services (OMES) includes the State's Chief Information Security Officer (CISO), the State's lead cybersecurity official, and Oklahoma Cyber Command, the State's cybersecurity division. In 2020, the OEMS created the Oklahoma Information Sharing and Analysis Center (OK-ISAC) to mitigate cybersecurity risks across Oklahoma by providing real-time monitoring, vulnerability identification, incident response and threat intelligence to its members and partners.

Oklahoma looks to create a cyber response team, including stakeholders from across the State and federal partners, to increase information sharing on cyber incidents. Further, Oklahoma seeks to enhance the role of the information technology service (ITS) unit within incident communications in the field.

Technology and cybersecurity goals and objectives include the following:

Technology and Cybersecurity	
Goal	Objectives
6. Increase information sharing on cyber incidents across the state (public and private sector)	6.1 Identify stakeholders from across the state (and including federal partners) to participate in cyber response team
	6.2 Host tabletop exercise with cyber response team to practice information sharing
	6.3 Log incidents in state WebEOC
7. Enhance the role of the ITS unit within incident communications in the field	7.1 Finalize All Hazards Public Safety Communications document to include the ITS unit portion
	7.2 Incorporate ITS unit positions into the incident management team

Technology and Cybersecurity	
Goal	Objectives
	7.3 Outreach and education of ITS unit capabilities
8. Establish integration requirements for LMR to LTE gateways	8.1 Create/identify proper working group
	8.2 Integrate new requirements into existing requirements
	8.3 Update existing requirements
9. Create a statewide LMR strategic plan	9.1 Work with the LMR Public Safety Interoperable Communications (PSIC) committee on technologies and requirements
	9.2 Increase LMR coverage in limited coverage areas
	9.3 Develop statewide LMR governance plan to incorporate all LMR systems across the state
10. Increase cohesion between the multiple islands of enhanced 9-1-1 deployment in the state and increased standardization of information and deployment	10.1 Enhance interoperability between PSAPs, including backups and fail over
	10.2 Require the entire state to have access to enhanced 9-1-1 services
	10.3 Review numbers of PSAPs across the state to enhance efficiency

FUNDING

Agencies outside metro areas face funding challenges in the transition to P25 Phase II, and local agencies have difficulty obtaining adequate funding for LMR. The State will focus on identifying funding requirements for public safety communications and grant opportunities.

Funding goals and objectives include the following:

Funding	
Goal	Objectives
11. Identify funding requirements for public safety communications	11.1 Coordinate with the LMR PSIC committee on technologies and requirements, the 9-1-1 authority, and other stakeholders

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 catalog³ of technical assistance available to assist with the implementation of the SCIP. Technical assistance requests are to be coordinated through the SWIC.

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

Goals	Objectives	Owners	Completion Date
1. Create an Alerts and Warnings guidance document for local government entities	1.1 Request TA for support	AMBER Alerts Committee, SWIC	December 2022
	1.2 Encourage the update of the state EAS plan		
	1.3 Weather service capability to issue evacuation orders		
2. Increase coordination between the SIGB and new governance bodies	2.1 Enhance continuity and collaboration between governance bodies	SIGB, SWIC	August 2023
3. Strengthen regional TICPs	3.1 Request CISA TA support	Sub Technology Group, SWIC	December 2022
4. Create a statewide P25 ID plan and strong MOU program	4.1 Create P25 ID/talkgroup plan working group to include representatives from each LMR system	System owners	August 2023
5. Finalize and disseminate state encryption plan	5.1 Coordinate with encryption working group	Encryption Working Group	August 2022
6. Increase information sharing on cyber incidents across the state (public and private sector)	6.1 Identify stakeholders from across the state (and including federal partners) to participate in cyber response team	State CISO	August 2022
	6.2 Host tabletop exercise with cyber response team to practice information sharing		
	6.3 Log incidents in state WebEOC		
7. Enhance the role of the ITS unit within incident communications in the field	7.1 Finalize All Hazards Public Safety Communications document to include the ITS unit portion	All Hazards Public Safety Communications Committee (AHPSCC), SWIC, Deputy SWIC	August 2023
	7.2 Incorporate ITS unit positions into the incident management team		
	7.3 Outreach and education of ITS unit capabilities		

³ [Emergency Communications Technical Assistance Planning Guide](#)

Goals	Objectives	Owners	Completion Date
8. Establish integration requirements for LMR to LTE gateways	8.1 Create/identify proper working group	System owners, Sub Technology Committee	Ongoing
	8.2 Integrate new requirements into existing requirements		
	8.3 Update existing requirements		
9. Create a statewide LMR strategic plan	9.1 Work with the LMR PSIC committee on technologies and requirements	LMR PSIC committee, system owners	June 2022
	9.2 Increase LMR coverage in limited coverage areas		
	9.3 Develop statewide LMR governance plan incorporate all LMR systems across the state		
10. Increase cohesion between the multiple islands of enhanced 9-1-1 deployment in the state and increased standardization of information and deployment	10.1 Enhance interoperability between PSAPs, including backups and fail over	9-1-1 Authority, State 9-1-1 Coordinator	August 2022
	10.2 Require the entire state to have access to enhanced 9-1-1 services		
	10.3 Review numbers of PSAPs across the state to enhance efficiency		
11. Identify funding requirements for public safety communications	11.1 Coordinate with the LMR PSIC committee on technologies and requirements, the 9-1-1 authority, and other stakeholders	LMR PSIC	June 2022

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 2021 assessment of their progress against the markers.

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: <input type="checkbox"/> Communications Champion/SWIC <input type="checkbox"/> LMR <input type="checkbox"/> Broadband/LTE <input type="checkbox"/> 9-1-1 <input type="checkbox"/> Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: <input type="checkbox"/> Communications Champion/SWIC <input type="checkbox"/> LMR <input type="checkbox"/> Broadband/LTE <input type="checkbox"/> 9-1-1 <input type="checkbox"/> Alerts, Warnings and Notifications	Optimized (5) 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"/> 9-1-1 <input checked="" type="checkbox"/> 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 >1, <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	<50% are strategic goals in SCIP	>50%<90% are strategic goals in SCIP	>90% are strategic goals in SCIP

	emergency communications ecosystem (LMR, LTE, 9-1-1, 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)			
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: <input checked="" type="checkbox"/> COML <input checked="" type="checkbox"/> COMT <input checked="" type="checkbox"/> ITSL <input checked="" type="checkbox"/> RADO <input checked="" type="checkbox"/> INCM <input checked="" type="checkbox"/> INTD <input checked="" type="checkbox"/> AUXCOM <input type="checkbox"/> 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	Interoperable communications SOPs/SOGs are formalized and in use by agencies within the area. Despite minor	Interoperable communications SOPs/SOGs within the area are formalized and regularly reviewed.

		these interoperability procedures among some agencies	issues, SOPs/SOGs are successfully used during responses and/or exercises	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	Field Operations Guides (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
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 of the four A&W characteristics	>50%<74% of originating authorities have all of the four A&W characteristics	>75%<100% of originating authorities have all of the four 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 programmed for interoperability and consistency	>50%<74% of radios are programmed for interoperability and consistency	>75%<100% of radios are programmed for interoperability and consistency
14	Cybersecurity Assessment Awareness. Cybersecurity assessment awareness.	Public safety communications network owners are aware of	Initial plus, conducted assessment, conducted risk	Defined plus, Availability of Cyber Incident Response Plan

	(Public safety communications networks are defined as covering: LMR, LTE, 9-1-1, and A&W)	cybersecurity assessment availability and value (check yes or no for each option) <input type="checkbox"/> LMR <input type="checkbox"/> LTE <input type="checkbox"/> 9-1-1/CAD <input type="checkbox"/> A&W	assessment. (check yes or no for each option) <input type="checkbox"/> LMR <input type="checkbox"/> LTE <input type="checkbox"/> 9-1-1/CAD <input type="checkbox"/> A&W	(check yes or no for each option) <input checked="" type="checkbox"/> LMR <input checked="" type="checkbox"/> LTE <input checked="" type="checkbox"/> 9-1-1/CAD <input checked="" type="checkbox"/> A&W
15	NG9-1-1 implementation. NG9-1-1 implementation underway to serve state / territory population.	Working to establish NG9-1-1 governance through state/territorial plan. <ul style="list-style-type: none"> • Developing GIS to be able to support NG9-1-1 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • Planning to or have updated PSAP equipment to handle basic NG9-1-1 service offerings. 	More than 75% of PSAPs and Population Served have: <ul style="list-style-type: none"> • NG9-1-1 governance established through state/territorial plan. • GIS developed and able to support NG9-1-1 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • PSAP equipment updated to handle basic NG9-1-1 service offerings. 	More than 90% of PSAPs and Population Served have: <ul style="list-style-type: none"> • NG9-1-1 governance established through state/territorial plan. • GIS developed and supporting NG9-1-1 call routing. • Operational Emergency Services IP Network (ESInet)/Next Generation Core Services (NGCS). • PSAP equipment updated and handling basic NG9-1-1 service offerings.
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 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.
17	Future Technology/Organizational Learning. SIEC/SIGB is tracking, evaluating, implementing future technology (checklist)	<input checked="" type="checkbox"/> LMR to LTE Integration <input checked="" type="checkbox"/> 5G <input checked="" type="checkbox"/> IoT (cameras) <input checked="" type="checkbox"/> UAV (Smart Vehicles) <input checked="" type="checkbox"/> UAS (Drones)	<input checked="" type="checkbox"/> Wearables <input type="checkbox"/> Machine Learning/Artificial Intelligence/Analytics <input checked="" type="checkbox"/> Geolocation <input checked="" type="checkbox"/> GIS	<input checked="" type="checkbox"/> HetNets/Mesh Networks/Software Defined Networks <input checked="" type="checkbox"/> Acoustic Signaling (Shot Spotter) <input checked="" type="checkbox"/> ESInet

		<input checked="" type="checkbox"/> Body Cameras <input checked="" type="checkbox"/> Public Alerting Software <input checked="" type="checkbox"/> Sensors <input checked="" type="checkbox"/> Autonomous Vehicles <input checked="" type="checkbox"/> MCPTT Apps	<input checked="" type="checkbox"/> Situational Awareness Apps-common operating picture applications (i.e. Force Tracking, Chat Applications, Common Operations Applications)	<input checked="" type="checkbox"/> 'The Next Narrowbanding' <input checked="" type="checkbox"/> Smart Cities
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%<100% 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%<100% 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	Initial plus web presence containing information about emergency communications	Defined plus in-person/webinar conference/meeting

		media, etc.) distributed to relevant stakeholders on regular basis	interoperability, SCIP, trainings, etc.	attendance strategy and resources to execute
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%<100% 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%<100% 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: <input type="checkbox"/> Governance <input type="checkbox"/> SOPs/MOUs <input type="checkbox"/> Technology <input type="checkbox"/> Training/Exercises <input type="checkbox"/> Usage	Defined: Documented/established across some lanes of the Continuum: <input type="checkbox"/> Governance <input type="checkbox"/> SOPs/MOUs <input type="checkbox"/> Technology <input type="checkbox"/> Training/Exercises <input type="checkbox"/> Usage	Optimized: Documented/established across all lanes of the Continuum: <input checked="" type="checkbox"/> Governance <input checked="" type="checkbox"/> SOPs/MOUs <input checked="" type="checkbox"/> Technology <input checked="" type="checkbox"/> Training/Exercises <input type="checkbox"/> Usage

APPENDIX B: ACRONYMS

Acronym	Definition
9-1-1 ACOG	9-1-1 Association of Central Oklahoma Governments
AAR	After-Action Report
AHPSCC	All Hazards Public Safety Communications Committee
AMBER	America's Missing: Broadcast Emergency Response
AUXCOMM/AUXC	Auxiliary Emergency Communications
A&W	Alerts and Warnings
CASM	Communication Assets Survey and Mapping
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
E9-1-1	Enhanced 9-1-1
EAS	Emergency Alert System
ECD	Emergency Communications Division
eFOG	Electronic Field Operations Guide
EOC	Emergency Operations Center
ESInet	Emergency Services Internal Protocol Network
FirstNet	First Responder Network Authority
FOG	Field Operations Guide
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information System
HSGP	Homeland Security Grant Program
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-RF Subsystem Interface
IT	Information Technology
ITS	Information Technology Service
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
MHz	Megahertz

Acronym	Definition
MOU	Memorandum of Understanding
NECP	National Emergency Communications Plan
NG9-1-1	Next Generation 9-1-1
ODEMHS	Oklahoma Department of Emergency Management and Homeland Security
OK-ISAC	Oklahoma Information Sharing and Analysis Center
OKWIN	Oklahoma Wireless Information Network
OMACS	Oklahoma Multiple Agency Communications System
OMES	Office of Management and Enterprise Services
PSAP	Public Safety Answering Point
PSIC	Public Safety Interoperable Communications
PTS	Priority Telecommunication Services
P25	Project 25
RADO	Radio Operator
SCIP	Statewide Communication Interoperability Plan
SIGB	Statewide Interoperable Governance Body
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