Oregon

Statewide Communications Interoperability Plan

August 2021

Developed by the Oregon State Interoperability Executive Council with Support from the Cybersecurity and Infrastructure Security Agency and Enterprise Information Services.

Version 1.1 (Updated November 2021)

THIS PAGE INTENTIONALLY LEFT BLANK

Revision Record

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	**08/2021**	**Baseline Document**
1.1	11/2021	Added Appendix B: Grant Guidance and Investment Priorities, and Appendix D: National Emergency Communications Plan Priorities. Acronym list moved to Appendix E.

TABLE OF CONTENTS

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

Greetings,

As the Statewide Interoperability Coordinator (SWIC) for the State of Oregon, I am pleased to present to you the 2021 Oregon Statewide Communication Interoperability Plan (SCIP). This SCIP represents Oregon's continued commitment to improving emergency communications interoperability and supporting the public safety practitioners and emergency managers throughout the state. In addition, this update meets the requirement of the current U.S. Department of Homeland Security (DHS) grant guidelines and the SIEC's mandate under Oregon Revised Statute 403.455.

Representatives from Oregon's State Interoperability Executive Council (SIEC) and its subcommittees collaborated with public safety, emergency management, cybersecurity, and emergency communications stakeholders from across the state 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 funding sustainability, and are designed to support our state in planning for new technologies and to assist with navigation of the ever-changing emergency communications ecosystem. They also incorporate the opportunities for improved interoperability identified by the State Interoperability Markers which describe Oregon's level of interoperability maturity by measuring the state's progress against 25 markers.

As we continue to enhance interoperability and embrace new technologies, we must remain dedicated to improving our ability to communicate among disciplines and across jurisdictional boundaries for the good of all Oregonians. With help from public safety and emergency management practitioners, emergency communications stakeholders, and our private sector partners statewide, we will work to achieve the goals set forth in this SCIP and become a nationwide model for statewide interoperability.

Sincerely,

William Chapman, ENP
Oregon SWIC

ENTERPRISE information services

INTRODUCTION

The Oregon SCIP is a one-to-three-year strategic planning document (updated annually) 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.
- **Vision and Mission** – Articulates Oregon'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 Oregon 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** – Outlines public safety technology and operations needed to maintain and enhance interoperability across the emergency communications ecosystem.
- **Funding Sustainability** – Describes the funding sources and allocations that support interoperable communications capabilities within Oregon along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan** – Describes Oregon's plan to implement, maintain, and update the SCIP to enable continued evolution of and progress toward the Oregon's interoperability goals.

The Emergency Communications Ecosystem (shown in Figure 1) 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 newly released 2019 National Emergency Communications Plan (NECP)[1].

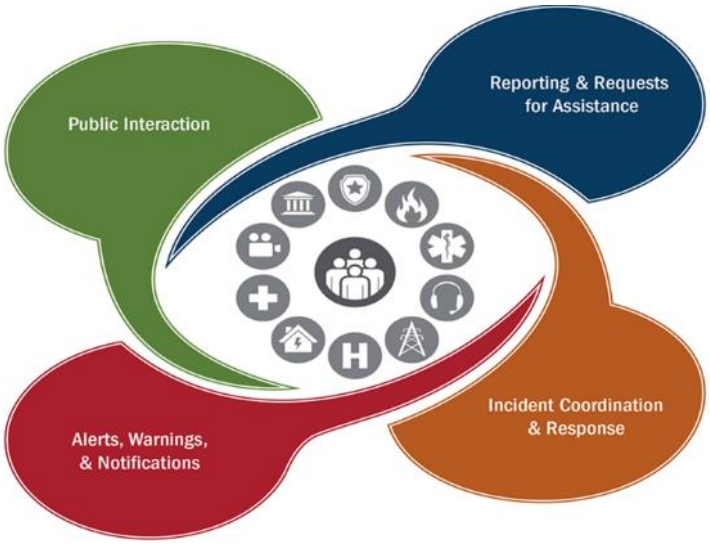

Figure 1: Emergency Communications Ecosystem

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

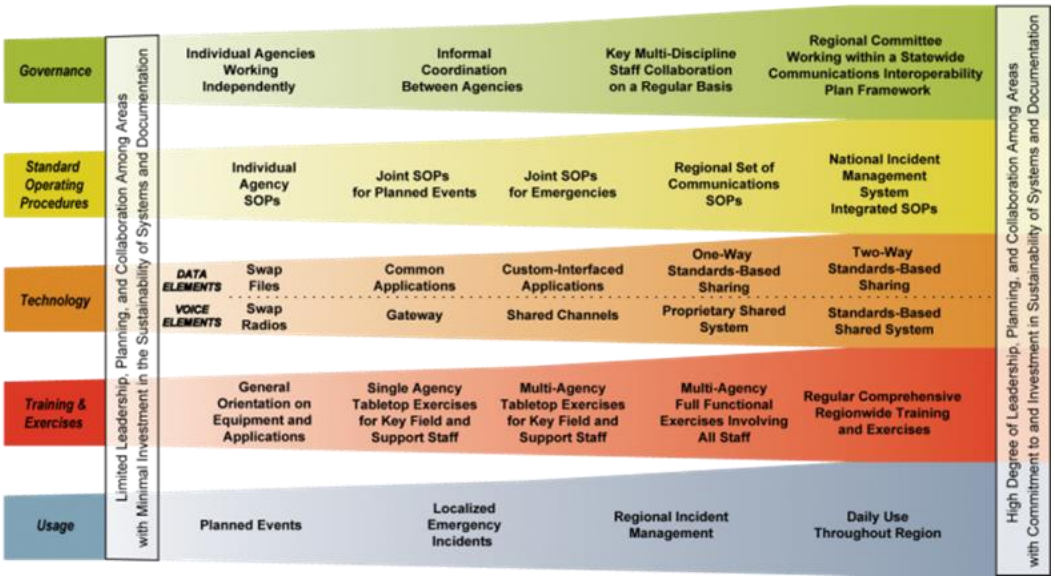

Figure 2: Interoperability Continuum

[1] The 2019 National Emergency Communications Plan is available here: https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_0.pdf.

[2] The Interoperability Continuum Brochure is available here: https://www.cisa.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf.

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 9-1-1 services have long been and continue to be critical tools for communications. However, the advancement of internet protocol (IP) 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.

An example of this evolution is the First Responder Network Authority's (FirstNet) implementation of the Nationwide Public Safety Broadband Network (NPSBN). Similarly, the transition of public-safety answering points (PSAPs) to Next Generation 9-1-1 (NG9-1-1) technology 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 Oregon's vision and mission for improving emergency and public safety communications interoperability:

Vision:

Seamless, interoperable, and resilient emergency communications

Mission:

Provide leadership, strengthen partnerships, and advocate for resources and investment in voice, data, 9-1-1, and public alerts interoperability

GOVERNANCE

State Interoperability Executive Council

The SIEC is established by the Oregon Revised Statutes (ORS) 403.450 under the State Chief Information Officer to be the statewide interoperability governing body serving as the primary steering group for the Oregon SCIP[3]. The membership of the Council consists of two members of the Legislative Assembly and representatives from the following agencies, organizations, and the public

- Department of State Police
- Office of Emergency Management
- Department of Forestry
- Department of Corrections
- Department of Transportation
- Office of the State Chief Information Officer
- Oregon Health Authority
- Oregon Military Department
- Department of Public Safety Standards and Training
- Broadband Advisory Council
- Tribal representative
- Public representative
- Fire Chief's Association
- Association of Chiefs of Police
- State Sheriffs Association
- Association of Oregon Counties
- League of Oregon Cities
- Special Districts Association of Oregon
- Technology officer of an Oregon city
- Technology officer of an Oregon county
- Representative of a nonprofit professional organization interested in the enhancement of public safety communications
- A member of the public who works or resides in Federal Communications Commission (FCC) Region 35

The SIEC consists of the following committees: Executive, Broadband, Partnership, Strategic Planning, and Technical. Each of the committees are chartered individually in their role and

[3] The duties of the SIEC are outlined in ORS 403.455 here: https://www.oregonlaws.org/ors/403.455

membership, and are representative of state, local, and tribal entities. The table below outlines the purpose of each committee.

Executive Committee	Comprised of the SIEC Chair and Vice-Chair along with the Chairs of all the other committees, the Executive Committee performs all functions and does all acts, between meetings, which the SIEC might do during regular meetings except for amending the SIEC Charter or SCIP
Broadband Committee	Assist in identifying the common interoperable framework to provide recommendations on, and help Oregon leverage, subsequent broadband assets and relationships
Partnership Committee	Maximize resource sharing and interoperability of communications
Strategic Planning Committee	Develop the framework of the SCIP, and monitor and report on the implementation of the Council's goals and objectives as well as assisting other committees in developing charters, goals, and objectives in support of the SCIP
Technical Committee	Serve as the technical research and advisory resource for the Council and ensure that all government agencies have the opportunity to participate in technical discussions and in formulating recommendations for the SIEC

Below is the organizational structure of the SIEC.

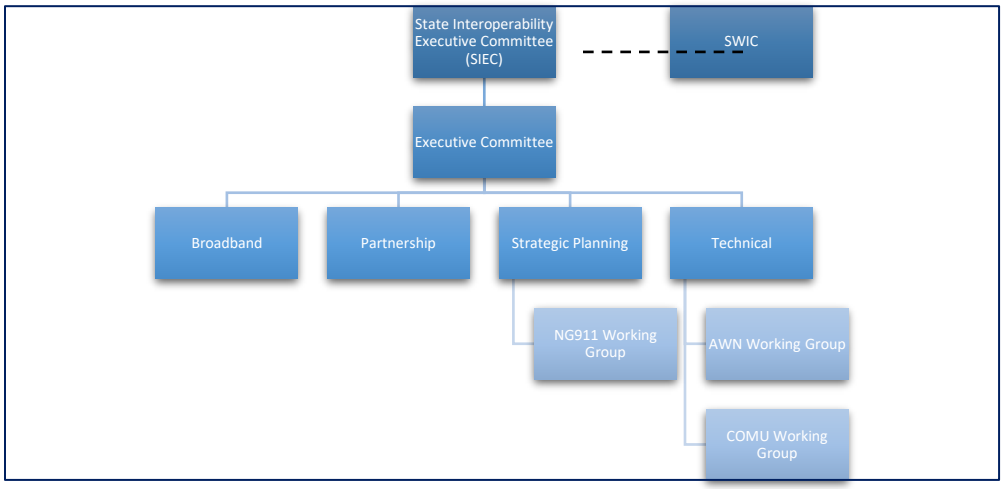

Figure 3: SIEC Organizational Structure

Governance Goals & Objectives	
Goal	**Objectives**
1. Increase engagement and awareness of interoperable communications	1.1 Develop an outreach, education, and listening engagement plan for local, county, tribal, and/or state elected leaders. 1.2 Conduct at least 2 outreach and education events targeting emergency communications stakeholders in support of interoperability best practices 1.3 Increase GETS/WPS subscriptions by 5% statewide 1.4 Develop a TSP Adoption Plan and cost analysis 1.5 Develop at least one Regional Interoperability Group

TECHNOLOGY

Current State

Land Mobile Radio

The State of Oregon has adopted a system of systems approach to interoperability. Local and regional radio systems have joined cooperatively to develop radio networks offering wide-area interoperability across much of the state. Some areas remain remote with limited connectivity to the rest of the state.

Mobile Broadband

The Governor of the State of Oregon opted into the buildout of the National Public Safety Broadband Network (FirstNet). Local, state, and tribal agencies are now evaluating the coverage and capabilities of FirstNet to see if it meets their agency mobile broadband business requirements.

As of August 2021, approximately 21,500 subscribers have adopted FirstNet in Oregon. 23 of the 45 site buildouts are complete which represents 51% of the Oregon RAN buildout per the state plan. The remaining 22 sites are in different stages of site acquisition and construction activities. Oregon has established an emergency resource request and escalation plan through the FirstNet Response Operations Group and State Emergency Coordination Center's Emergency Support Function (ESF) – 2 (Communications). This plan has been exercised on multiple real-world emergencies. The FirstNet team in Oregon, in collaboration with the Statewide Interoperability Program have deployed assets to support first responders during fires, winter storms and in response to the COVID-19 emergencies effectively. Currently, site resiliency and coverage in rural areas of Oregon are the primary focus, in addition to completing the RAN buildout on schedule.

Other Tier 1 carriers remain widely deployed throughout public safety. Coverage remains the top priority for agencies.

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

The State 9-1-1 Program is managed by the Oregon Office of Emergency Management (OEM) and its purpose is to plan, implement, administer, operate, and maintain the emergency communications system required to fulfill the requirements of ORS 403.115.

Currently, 9-1-1 services are funded in part through the Emergency Communications Tax and has a sunset date of December 31, 2030. Additionally, the State Chief Information Officer (CIO) has recommended that OEM develop and implement a Strategic NG9-1-1 Plan.

There are currently 43 PSAPs across 36 counties within the State.

Alerts and Warnings

In October 2020, the State of Oregon Legislative Emergency Board provided funding for a statewide emergency notification system based on a goal within the 2020 SCIP. In January of 2021, the State of Oregon rolled out a statewide alerts and warning system known as OR-Alert based upon the Everbridge platform. The system is provided to all counties and tribes for the distribution of emergency alerts, warnings, and notifications across a variety of communications pathways including SMS text, voice calls, IPAWS, and a mobile application, and can be accessed by the public via a shared website at www.oralert.gov . The system is governed by the OR-Alert Governance Committee, a working group of the SIEC Technical Committee. OR-Alert is capable of alerting across the state as of January 2021 through the Oregon Office of Emergency Management. County deployments are ongoing and are scheduled to be substantially complete by 4th quarter 2021. Malheur and Umatilla counties have opted out of the OR-Alert system but maintain substantially similar alerting software platforms.

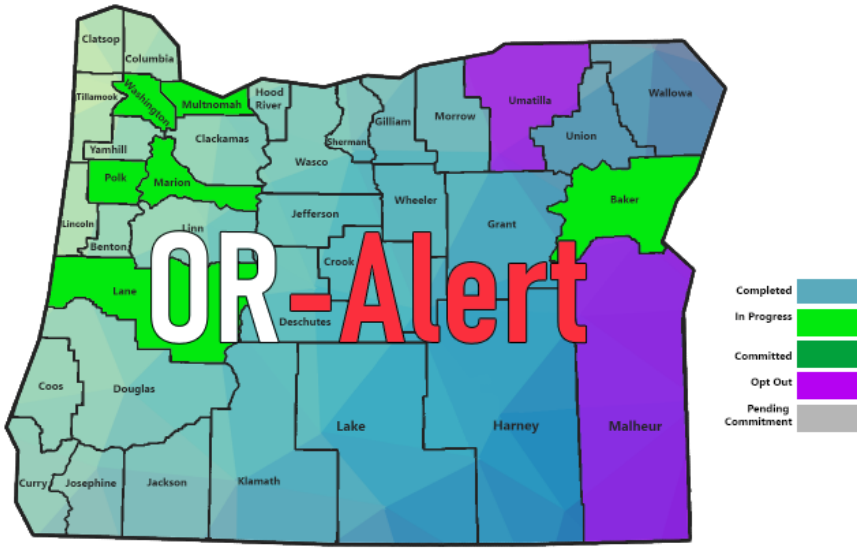

Figure 4: OR-Alert Deployment as of 08/09/21

The Oregon State Police (OSP) are responsible for disseminating Amber Alerts while OEM facilitates the dissemination of statewide emergency alerts. The Oregon State Emergency Alert System Plan[4] outlines the organization and implementation of the State of Oregon Emergency Alert System (EAS) and is administrated by the Oregon State

[4] The Oregon EAS Plan is available here: https://www.fcc.gov/files/oreasplan2017docx.

Emergency Communications Committee (SECC). In addition, there are 29 state and local organizations that have received Integrated Public Alert and Warning System (IPAWS) authority or are in the process of becoming IPAWS Alerting Authorities.

Technology Goals & Objectives	
Goal	**Objectives**
2. Adopt NG-911 in Oregon	2.1 Complete roadmap of NG-911 Strategic Plan 2.2 Develop a Strategic NG-911 Plan
3. Develop and promote awareness of statewide guidance on interoperable communications.	3.1 Update FOG and conduct end user training 3.2 Develop and adopt statewide guidance for alerts and warnings. 3.3 Develop a white paper on FirstNet's proposed push-to-talk solutions to include a cost benefit analysis, reliability, and interoperability potential 3.4 Conduct at least one cybersecurity tabletop exercise 3.5 At least 10 public safety communications organizations participate in CISA Cyber Security Technical Assistance offerings. 3.6 Promote the adoption of the State of Oregon whole Community Cyber Disruption Plan. 3.7 Develop a plan for the use of federal and non-federal interoperability channels 3.8 Develop statewide Interoperable communications grant guidance and investment priorities
4. Document statewide LMR System of Systems	4.1 Document border states communications issues and solutions 4.2 Document performance of 2 radio systems' ISSI roaming capabilities 4.3 Develop a graphic describing radio system across the state. 4.4 Assess and document resilient EOC-to-EOC communications

TRAINING AND EXERCISES

Oregon is prioritizing the implementation of an all-hazards approach to incident communications and has developed a process for the training, certification, and credentialing of Communications Unit (COMU) resources throughout the state. It is critically important that these trained personnel have the opportunity to practice their skills in a real-world setting and complete their position task books. The SIEC supports the inclusion of emergency communications and the COMU in exercises and training events across the state.

Training and Exercises Goals & Objectives	
Goal	**Objectives**
5. Support COMU program and Improve Communications Response Capability	5.1 Hold one INCM Course 5.2 Hold one COMT Course 5.3 Hold one ITSL Course 5.4 Identify COML Management Training 5.5 Begin recognition of personnel 5.6 Develop long-term program maintenance strategy 5.7 Hold State COMU Exercise 5.8 Hold workshop for large system managers on the COMU Program and integration of All-Hazards Personnel 5.9 Develop an awareness and outreach plan for the COMU 5.10 Increase the number of 7/800 MHz subscriber radios available in caches and on Mobile Communications Vehicles 5.11 Develop gateway like capability for the Strategic Technology Reserve

FUNDING AND SUSTAINABILITY

Current State of Funding

The Enterprise Information Services operational budget includes funding for the SWIC, Deputy SWIC, Public Safety Communications Specialist, and an Assistant State CIO for Public Safety, as well as technical, project, and conference support for the SIEC.

Funding and Sustainability Goals & Objectives

Goal	Objectives
6. Advocate for continued funding of the SIEC and the Statewide Interoperability Program	6.1 Produce and distribute report on success of the SIEC to SIEC members for distribution to larger audience. 6.2 Develop a financial plan for the next biennium

IMPLEMENTATION PLAN

Goal	Objectives	Champions	Start Date	Completion Date	Comments / Impact
1. Increase engagement and awareness of interoperable communications	1.1 Develop an outreach, education, and listening engagement plan for local, county, tribal, and/or state elected leaders.	SWIC	On adoption of the SCIP.	Dec-21	
	1.2 Conduct at least 2 outreach and education events targeting emergency communications stakeholders in support of interoperability best practices	Partnership Committee	On adoption of the SCIP.	Dec-22	
	1.3 Increase GETS/WPS subscriptions by 5% statewide	Priority Telecommunications Services (PTS) Area Representative	On adoption of the SCIP.	Aug-22	As measured by CISA
	1.4 Develop a TSP Adoption Plan and cost analysis	SWIC	On adoption of the SCIP.	Dec-21	
	1.5 Develop at least one Regional Interoperability Group	Partnership Committee	On adoption of the SCIP.	Aug-22	
2. Adopt NG-911 in Oregon	2.1 Complete roadmap of NG-911 Strategic Plan	NG-911 Working Group	On adoption of 21 SCIP	Dec-21	
	2.2 Develop a Strategic NG-911 Plan	NG-911 Working Group	Aug-20	Jun-22	Enterprise Information Services

					Strategic Framework[1] assigns a June 30, 2022 deadline for developing the Plan. NG-911 working group is working with OEM and EIS on plan and role of committee.
3. Develop and promote awareness of statewide guidance on interoperable communications.	3.1 Update FOG and conduct end user training	SWIC	On adoption of 21 SCIP	Dec-21	
	3.2 Develop and adopt statewide guidance for alerts and warnings.	OR-Alert Governance Committee	On adoption of 21 SCIP	Jun-22	
	3.3 Develop a white paper on FirstNet's proposed push-to-talk solutions to include a cost benefit analysis, reliability, and interoperability potential	Technical Committee, Single Point of Contact (SPOC),	On adoption of 21 SCIP	Dec-21	
	3.4 Conduct at least one cybersecurity tabletop exercise	CISA Cybersecurity Advisor (CSA)	On adoption of 21 SCIP	Sep-22	
	3.5 At least 10 public safety communications organizations participate in CISA Cyber Security Technical Assistance offerings.	CISA Cybersecurity Advisor (CSA)	On adoption of 21 SCIP	Sep-22	

	3.6 Promote the adoption of the State of Oregon whole Community Cyber Disruption Plan.	Cybersecurity Services	On adoption of 21 SCIP	Ongoing	
	3.7 Develop a plan for the use of federal and non-federal interoperability channels	Technical Committee, SWIC	On adoption of 21 SCIP	May-22	
	3.8 Develop statewide Interoperable communications grant guidance and investment priorities	Technical Committee	On adoption of 21 SCIP	Dec-21	
4. Document statewide LMR System of Systems	4.1 Document border states communications issues and solutions	Technical Committee	Jan-22	04/01/222	
	4.2 Document performance of 2 radio systems' ISSI roaming capabilities	Technical Committee	Sep-21	Jun-22	Report should contain top 5 successes and issues/limitations
	4.3 Develop a graphic describing radio systems across the state.	Technical Committee	Sep-21	Jun-22	
	4.4 Assess and document resilient EOC-to-EOC communications	OEM	On adoption of SCIP	Aug-22	
5. Support COMU program and Improve	5.1 Hold one INCM Course	SWIC	On adoption of SCIP	Oct-21	

Communications Response Capability	5.2 Hold one COMT Course	SWIC	On adoption of SCIP	Jun-22	
	5.3 Hold one ITSL Course	SWIC	On adoption of SCIP	Jun-22	
	5.4 Identify COML Management Training	SWIC	On adoption of SCIP	Jun-22	
	5.5 Begin recognition of personnel	COMU Working Group	On adoption of SCIP	Ongoing	
	5.6 Develop long-term program maintenance strategy	COMU Working Group, Executive Committee	Oct-21	Jun-22	
	5.7 Hold State COMU Exercise	COMU Working Group, SWIC	Jan-22	Apr-22	
	5.8 Hold workshop for large system managers on the COMU Program and integration of All-Hazards Personnel	COMU Working Group, SWIC	Oct-21	Apr-22	
	5.9 Develop an awareness and outreach plan for the COMU	COMU Working Group	Jan-22	Dec-22	
	5.10 Increase the number of 7/800 MHz subscriber radios available in caches and on Mobile Communications Vehicles	COMU Working Group	On adoption of the SICP	Dec-24	

	5.11 Develop voice-gateway like capability for the Strategic Technology Reserve.	Technical Committee	On adoption of the SICP	Dec-24	
6. Advocate for continued funding of the SIEC and the Statewide Interoperability Program	6.1 Produce and distribute report on success of the SIEC to SIEC members for distribution to larger audience.	Executive Committee	On adoption of SCIP	Dec-21	
	6.2 Develop a financial plan for the next biennium	Executive Committee, Strategic Planning Committee	On adoption of SCIP	May-22	

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 Oregon's assessment of their progress against the markers.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
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 ☐ 9-1-1 ☐ Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 9-1-1 ☐ Alerts, Warnings and Notifications	Optimized (5) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 9-1-1 ☒ Alerts, Warnings and Notifications	SIEC should consider adding representatives from OSFM and OEMA.
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 emergency communications ecosystem (LMR, LTE, 911, A&W) and	<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	Comments
	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	SIEC needs to provide clear grant guidance for equipment selections made using grant dollars.
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	

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
				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	In progress but not yet complete. State did complete FEMA ESF-2 annex including an inventory of state and regional assets.
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	In progress but not yet complete.
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	OR-Alert implementation in progress. SIEC AWN Working group established.
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%<100% of radios are programed for interoperability and consistency	Smaller agencies may have inconsistent naming conventions/unable to access interop channels. Difficult to measure.
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 ☒ 9-1-1 / CAD	Initial plus, conducted assessment, conducted risk assessment. (check yes or no for each option) ☐ LMR ☐ LTE ☐ 9-1-1 / CAD	Defined plus, Availability of Cyber Incident Response Plan (check yes or no for each option) ☐ LMR ☐ LTE ☐ 9-1-1 / CAD	Awareness is low for LTE/LMR. Better for 9-1-1/CAD and A&W. Statewide Cyber Disruption Plan in final draft.

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
		☒ A&W	☐ A&W	☐ 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.	More than 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 Next Generation Core Services (NGCS). • PSAP equipment updated to handle basic NG911 service offerings.	More than 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)/Next Generation Core Services (NGCS). • PSAP equipment updated and handling basic NG911 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.	The state provides OpsCenter to ALL state agencies and local/tribal jurisdictions. RAPTOR GIS platform is available and authorized users are able to provide and share information. Some regions have achieved CAD-To-CAD Interoperability. Statewide implementation of supplementation location information delivery and the ability to acquire additional data in progress for all PSAPs.
17	**Future Technology/Organizational Learning.** SIEC/SIGB is tracking, evaluating, implementing future technology (checklist)	☒ LMR to LTE Integration ☒ 5G ☒ IoT (cameras) ☒ UAV (Smart Vehicles) ☒ UAS (Drones) ☒ Body Cameras ☒ Public Alerting Software ☒ Sensors			

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
		☐ Autonomous Vehicles ☒ MCPTT Apps ☒ Wearables ☐ Machine Learning/Artificial Intelligence/Analytics ☒ Geolocation ☒ GIS ☒ Situational Awareness Apps-common operating picture applications (i.e. Force Tracking, Chat Applications, Common Operations Applications) ☒ HetNets/Mesh Networks/Software Defined Networks ☐ Acoustic Signaling (Shot Spotter) ☒ ESInet ☐ 'The Next Narrowbanding' ☒ 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	The state conducts regular communications exercises and regularly includes operational communications as exercise evaluation components. FirstNet has developed a large library of injects for COMEXs. State also has access to COMEX portal.
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	OSFM and ODF have COMU Personnel available for statewide deployment. State COMU Program established but will take time to certify/credential new responders. Large systems need to be involved in working with COMU responders. Consider

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
					measuring through PTB completion.
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	Move to optimized
21	**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 7,968 GETS (12.68%) 3,666 WPS Subscribers (5.83%)	>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	PAR for the West Sector is located in OR. GETS - 6760 WPS – 2953
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	
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	For SCIP considerations, also consider local/regional systems and privately owned (LTE) networks.
24	**Risk identification.** Identify risks for emergency communications components.	<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	

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized	Comments
	(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)				
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: GRANT GUIDENCE AND INVESTMENT PRIORITIES

In accordance with ORS 403.455 (Duties of council), the SIEC is responsible for recommending to the Governor investments by the State of Oregon in public safety communications systems. Additionally, the SIEC is tasked to coordinate state, local and, as appropriate, tribal and federal activities related to obtaining federal grants for support of interoperability. To fulfill this duty, and to move the state towards the SIEC's vision of "Seamless, interoperable, and resilient emergency communications," the SIEC has established priorities for investment in emergency communications systems and provides the following recommended guidance for use by federal, state, and local grant administrators when determining awards related to communications.

Agencies are strongly encouraged to use the SAFECOM Guidance on Emergency Communications Grants Suggested Actions and Best Practices for Use during Grant Cycle Phases to assist with planning for communications grant applications.

Phases	Suggested Actions / Best Practices
Pre-Award	• Review and understand the NECP, SCIP, and other applicable plans • Coordinate with the SWIC and other key governance bodies and leadership to document needs, align projects to plans, and identify funding options[67] • Work with SAA to include projects in state preparedness plans and to secure funding • Review program requirements included in grant guidance • Consult the federal granting agency, spectrum authority (i.e., FCC or FirstNet Authority), and *SAFECOM Guidance* when developing projects • Align projects to federal and state-level plans and initiatives • Include coordination efforts with the whole community in applications • Identify staff to manage financial reporting and programmatic compliance requirements • Develop project and budget milestones to ensure timely completion • Identify performance measures and metrics that will help demonstrate impact • Consider potential impacts of EHP requirements on implementation timelines • Ensure proper mechanisms are in place to avoid commingling and supplanting of funds • Evaluate the ability of sub-recipients to manage federal funding • Consider how the project will be sustained after grant funding has ended
Award	• Review award agreement to identify special conditions, budget modifications, restrictions on funding, pass-through and reporting requirements, and reimbursement instructions • Update the proposed budget to reflect changes made during review and award • Inform sub-recipients of the award and fulfill any pass-through requirements
Post Award	• Establish repository for grant file and related data to be collected and retained from award through closeout, including correspondences, financial and performance reports, project metrics, documentation of compliance with EHP requirements and technology standards • Ensure fair and competitive procurement process for all grant-funded purchases • Understand the process for obtaining approval for changes in scope and budget • Adhere to proposed timeline for project and budget milestones; document and justify any delays impacting progress or spending • Leverage federal resources, best practices, and technical assistance • Complete financial and performance reports on time • Draw down federal funds as planned in budget milestones or in regular intervals • Complete projects within grant period of performance
Closeout	• Ensure all projects are complete • Maintain and retain data as required by the award terms and conditions • File closeout reports; report on final performance

Investment Priorities

National Emergency Communications Plan (NECP) Priorities

The SIEC fully supports the 6 national priorities identified in the National Emergency Communication Plan (NECP) and has included a general overview and examples of projects as Appendix D. Agencies should review the NECP and SAFECOM Grant Guidance and ensure projects align with national goals and priorities.

SIEC Investment Priorities

In addition to priorities outlined in the NECP, the SIEC specifically recommends the state make investments in projects that address the following areas:

- Hardening/Increasing resiliency of Communications (and dependent) Infrastructure. This may include:
  - Installation of security infrastructure such as fences, cameras, and alarm systems
  - Insulation of generators, batteries, solar systems, and fuel tanks allowing for a minimum of five days of utility disruption
  - Making sites seismically resilient in accordance with the current Oregon Structural Specialty code for essential facilities.
  - Installation of redundant backhaul connectivity at strategic sites
- Dual/tri band mobile/portable radio equipment for frontline responders and dispatch centers
- Caches of dual/tri band radios for use during a disaster, terrorist attack, or large-scale emergency.
- Deployable communications equipment including tactical repeaters, gateways, antennas, power systems, satellite connectivity, 3GPP Standards capable broadband devices, and associated accessories.

- Communications Staff, including dedicated positions responsible for coordination of regional communications efforts and interagency communications, as well as communications between PSAPs/Public Safety Dispatch Centers, EOCs, and other critical facilities.
- Funding subsequent phases of multi-phased projects previously funded and successfully carried out.
- Funding for Next Gen 911 planning, implementation, and deployment.
- Continued funding of OR-Alert.
- Continued funding of the SIEC and the Statewide Interoperability Program
- Refurbishment, update, and maintenance of the State's Strategic Technology Reserve, as well as funding for training and exercise related to use of the Reserve.
- Continued funding of the State Preparedness and Incident Response Equipment (SPIRE) grant program with expanded eligibility for communications equipment.
- Projects that increase cyber resilience of public safety communications networks and systems including implementation of cybersecurity measures identified in a formal system assessment or cybersecurity plan.

Funding Priority Recommendations

- When limited funding is available or funding is available through a competitive process, funding priority should be given to projects that have a statewide/interstate impact, followed by projects that have a regional/multi-agency impact. Lowest priority should be given to projects that only affect a single agency. Priority should also be given to projects that leverages or expands existing infrastructure, either through the state or regionally, whenever possible.

Funding Requirement Recommendations

It is the SIEC's recommendation that grant funding of any communication project should include:

- Coordination with the SWIC
- Coordination with SIEC's Technical Committee (for equipment purchases or infrastructure projects)
- Identification of the project in a jurisdiction or Region's Strategic Communications Plan
- Demonstrate that a lifecycle funding plan has been identified for any equipment/infrastructure investments.
- Full project plan with timelines, budget, and milestones identified.

Exclusions

The SIEC recommends that projects in the following categories be excluded from grant funding or other investment eligibility:

- Alerting Software that duplicates the capabilities provided to counties, tribes, and state agencies through the OR-Alert program.

  - This exclusion does not apply to capabilities that are outside the scope or OR-Alert or that expand the capabilities of OR-Alert. Ex: EAS hardware, devices capable of receiving alerts, siren systems, visible messaging systems, etc.
  - This exclusion does not apply if OR-Alert does not meet a county's needs as determined by the grant administrating agency or the funding body.
  - To the extent possible, investments in alerting infrastructure should be compatible with OR-Alert and be capable of receiving and/or transmitting in Common Alerting Protocol (CAP).
  -

- Equipment or services offered by certain telecommunications providers identified in the John S. McCain National Defense Authorization Act of 2019, current SAFECOM Guidance on Emergency Communications Grants or any applicable notice of funding opportunities.

Resources

- SAFECOM guidance on Emergency Communications Grants
- National Emergency Communications Plan
- Roadmap to the Envisioned State of Emergency Communications
- SAFECOM FAQ: Understanding Project 25 Standards and Compliance
- List of Federal Financial Assistance Programs Funding Emergency Communications – October 21, 2021
- NECP Frequently Asked Questions
- Oregon State Preparedness and Incident Response Equipment (SPIRE) Grant Program
- Oregon Emergency Management Performance Grant (EMPG) Program
- Oregon Homeland Security Grant Program
- Assistance to Firefighters Grant Program
- Tribal Homeland Security Grant
- Port Security Grant

APPENDIX C: 2017 ORS 403.455

The State Interoperability Executive Council created under ORS 403.450 (State Interoperability Executive Council) shall:

(1) Develop, annually update and monitor implementation of the Oregon Statewide Communication Interoperability Plan, the goal of which is to achieve statewide interoperability of public safety communications systems. To the maximum extent possible, the Oregon Statewide Communication Interoperability Plan shall align with and support the Enterprise Information Resources Management Strategy described in ORS 276A.203 (State Chief Information Officer). As part of the executive council's duties under this subsection, the executive council shall:

(a) Recommend strategies to improve public safety communications interoperability among state, local, tribal and federal public safety agencies;

(b) Develop standards to promote consistent design and development of public safety communications infrastructures and recommend changes in existing public safety infrastructures that are necessary or appropriate for implementation of the interoperability plan;

(c) Identify immediate short-term technological and policy solutions to tie existing public safety communications infrastructures together into an interoperable communications system;

(d) Develop long-term technological and policy recommendations to establish a statewide public safety communications system to improve emergency response and day-to-day public safety operations; and

(e) Develop recommendations for legislation and for the development of state and local policies that promote public safety communications interoperability in this state.

(2) Recommend to the Governor, for inclusion in the Governor's budget, investments by the State of Oregon in public safety communications systems.

(3) Coordinate state, local and, as appropriate, tribal and federal activities related to obtaining federal grants for support of interoperability and request technical assistance related to interoperability.

(4) Conduct and submit an annual update of the interoperability plan to the United States Department of Homeland Security, Office of Emergency Communications, aligning the update with standards established in the National Emergency Communications Plan and by the federal office.

(5) Coordinate statewide interoperability activities among state, local and, as appropriate, tribal and federal agencies.

(6) Advise the State Chief Information Officer, the Governor and the Legislative Assembly on implementation of the interoperability plan.

(7) Serve as the Governor's Public Safety Broadband Advisory Group.

(8) Report to the Joint Committee on Ways and Means or to the Joint Interim Committee on Ways and Means, and to the Joint Legislative Committee on Information Management and Technology, on or before February 1 of each odd-numbered year, on the development of the interoperability plan and the executive council's other activities.

(9) Adopt rules necessary to carry out the executive council's duties and powers. [Formerly 401.872; 2010 c.107 §60; 2014 c.87 §6; 2015 c.807 §49; 2016 c.117 §61]

APPENDIX D: NATIONAL EMERGENCY COMMUNICATIONS PLAN (NECP) PRIORITIES

Governance & Leadership (NECP) Activities including:

- Funding of SIEC or Regional Interoperability Groups' activities
- Formation of Regional Interoperability Groups
- Other investments in emergency communications governance and leadership structures for coordinating statewide and regional initiatives that reflect the evolving emergency communications environment
- Outreach and education efforts
- Review and updating of key documents related to emergency communications, including charters, policies, procedures, and agreements to address new technologies

Planning & Procedures

- Update SCIPs, Regional Interoperability Group Plans documents, Tactical Interoperable Communications Plans (TICPs) and other strategic plans, and procedures to:
    - Support statewide and regional emergency communications and preparedness planning efforts through allocation of funding to the following planning activities:
    - Conduct and attend planning meetings
    - Engage the whole community in emergency communications planning, response, and risk identification
    - Develop and perform risk, resiliency, and vulnerability assessments (e.g., cyber, Threat and Hazard Identification and Risk Assessment [THIRA], communications security [COMSEC]
    - Incorporate risk management strategies for cybersecurity, continuity, and recovery (e.g., National Risk Index [NRI])
    - Integrate emergency communications assets and needs into state-level, regional, and county plans
- Coordinate with SWIC, State Administrative Agency (SAA), and state-level planners (e.g.,911 planners, utilities commissions) to ensure proposed investments align to statewide plans and comply with technical requirements
- Establish a cybersecurity response plan including continuity of vulnerable communications components and implementing resilient network designs (e.g., segmenting essential functions, strong access controls, two-factor authentication for staff logins) to limit the impact of cyber incidents.
- Identify, review, establish, and improve SOPs in coordination with response agencies at all levels of government to:
    - Ensure federal, state, local, tribal, and territorial roles and responsibilities are clearly defined

- Ensure communications assets and capabilities are integrated, deployed, and utilized to maximize interoperability
- Address threats, mitigate vulnerabilities, and identify contingencies for the continuity of critical communication

Training, Exercise, and Evaluation

- Conduct National Incident Management System (NIMS)-compliant training (e.g., training in:
    - Incident Command System [ICS] and the ICS Communications Unit such as:
        - Communications Unit Leader [COML],
        - Communications Technician [COMT],
        - Radio Operator [RADO],
        - Incident Tactical Dispatcher [INTD],
        - Auxiliary Communications [AUXCOMM], and
        - Incident Communication Center Manager [INCM])
        - Information Technology Services Unit Leader [ITSL]
        - Incident Tactical Dispatcher [INTD]
- Conduct frequent training and exercises involving personnel from all levels of government who are assigned to operate communications capabilities, to test communications systems and personnel proficiency (e.g., include emerging technologies and system failure), and utilize third party evaluators with communications expertise
- Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel, to ensure that responders effectively use and are not overloaded by available information
- Perform exercises that support and demonstrate the adoption, implementation, and use of the NIMS concepts and principles
- Hold cross-training and state, regional, or national level exercises to validate plans and procedures to include tribes, nongovernmental organizations, and public sector communications stakeholders
- Provide training and exercises on new and existing systems, equipment, and SOPs
- Develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, use of federal and national interoperability channels, personally identifiable information, and continuity of communications
- Test communications survivability, resilience, and continuity of communications, to include validation of continuity procedures and operational testing of backup systems and equipment
- Develop and support instructor cadres to expand training for communications-support personnel
- Assess and update training curriculums and exercise criteria to reflect changes in the operating environment and plain language protocols

- Identify opportunities to integrate private and public sector communications stakeholders into training and exercises, as well as cost-effective approaches (e.g., distance learning)
- Offer cybersecurity training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to guard against attacks
- Provide regular training and exercises for Alerting Authorities incorporating the use of IPAWS and OR-Alert

Communications Coordination

- Promote projects that confirm NIMS implementation, integrate members of the All-Hazards COMU Program, support continued use of ICS, and promote information sharing
- Establish or enhance primary, secondary, and backup communications capabilities and share appropriate ICS forms and information illustrating the status of an agency's capabilities
- Assess and improve the timeliness of notification, activation, and response of communications systems providers to support the Incident Commander, Incident Management Team(s), and EOC's requirements at incidents and planned events
- Enhance the coordination and effective usage of communications resources
- Ensure inventories of emergency communications resources are updated and comprehensive, and readily share information about features, functionality, and capabilities of operable and interoperable communication resources with partners o Promote assessment of communications assets, asset coordination, and resource sharing
- Implement projects that promote regional, intra- and inter-state collaboration
- Support initiatives that engage the whole community, including commercial and nontraditional communications partners (e.g., auxiliary communications, volunteers, utilities)
- Develop or update operational protocols and procedures
- Develop, integrate, or implement NIMS aligned SOPs to facilitate the integration, deployment, and use of communications assets
- Test communications capabilities and personnel proficiency through training, exercises, and real-world events and address needs identified in statewide plans, AARs, or assessments through comprehensive action plans
- Develop recommended guidelines regarding the use of personal communications devices (e.g., bring your own device) for official duties based on applicable laws and regulations
- Review usage of Priority Telecommunications Services (e.g., Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority), and ensure SOPs govern the programs' use, execution, and testing
- Plan for Alerting Authorities to ensure the highest state of readiness of OR-Alert for resilient and interoperable alerts, warnings, messaging and notifications

- Review uses of the NPSBN, also known as FirstNet, and other public safety broadband capabilities, and ensure SOPs govern the programs' use, execution, and testing
- Strengthen resilience and continuity of communications
- Inventory and typing of resources and other activities that strengthen resilience and provide backup communications solutions (e.g., radio caches, cell on wheels [COWs])
- Establish testing and usage observations of primary, secondary, and backup communications
- Address system and staffing for continuity of operations planning

Technology and Infrastructure

- Sustain and maintain current LMR capabilities based on mission requirements
- Purchase and use P25 compliant LMR equipment (see P25 Compliance Assessment Program [CAP] approved equipment list) for mission critical voice communications
- Support rapid and far-ranging deployment of the NPSBN and use of FirstNet devices and applications dedicated for public safety using multi-layered, proven cybersecurity and network security solutions
- Transition towards NG911 capabilities in compliance with NG911 standards
- Support standards that allow for alerts, warnings, and notifications across different systems
- Secure and protect equipment, information, and capabilities from physical and virtual threats
- Employ standards-based information exchange models and data sharing solutions
- Secure standards-based interconnectivity gateway subsystems
- Sustain and ensure critical communication systems connectivity and resiliency, including backup solutions, among key government leadership, internal elements, other supporting organizations, and the public under all conditions
- Support standards and practices that enhance survivability and resilience to electromagnetic effects
- Ensure all communications systems and networks are traced from end-to-end to identify all Single Points of Failure, including redundancy at critical infrastructure facilities, and:
    - Sustain availability of backup systems (e.g., backup power, portable repeaters, satellite phones, High Frequency [HF] radios)
    - Ensure diversity of network element components and routing
    - Plan for geographic separation of primary and alternate transmission media
    - Maintain spares for designated critical communication systems
    - Work with commercial suppliers to remediate single points of failure
    - Maintain communications capabilities to ensure their readiness when needed

Cybersecurity

- Develop and maintain cybersecurity risk management
- Implement the CISA Cyber Essentials Toolkits
- Implement the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to complement an existing risk management process or to

develop a credible program if one does not exist. The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including:
    - Identify, evaluate, and prioritize risks
    - Protect against identified risks
    - Detect risks to the network as they arise
    - Deploy response capabilities to mitigate risks
    - Establish recovery protocols to ensure the resiliency and continuity of communications
- Perform a Cyber Resilience Review
- Employ the Cyber Resiliency Resources available for public safety
- Identify and implement standards for cybersecurity that fit system and mission needs while maintaining operability and interoperability
- Develop incident response plans, recovery plans, resiliency plans, and continuity of operations plans in anticipation of physical or cybersecurity incidents
- Mitigate cybersecurity vulnerabilities with consideration of potential impacts of cybersecurity risk management on interoperability with the broader community
- Identify and mitigate equipment and protocol vulnerabilities

APPENDIX E: ACRONYMS

Acronym	Definition
COMU	Communications Unit
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cybersecurity Advisor
CSS	Cyber Security Services
DHS	United States Department of Homeland Security
EAS	Emergency Alert System
EOC	Emergency Operations Center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FirstNet	First Responder Network Authority
GETS	Government Emergency Telecommunications Service
IP	Internet Protocol
FOG	Field Operations Guide
IPAWS	Integrated Public Alert & Warning System
ISSI	Inter-RF Subsystem Interface
LMR	Land Mobile Radio
MHz	Megahertz
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NPSBN	National Public Safety Broadband Network
OEM	Office of Emergency Management
ORS	Oregon Revised Statutes
OSCIO	Office of the State Chief Information Officer
OSP	Oregon State Police
PSAP	Public Safety Answering Point
PTS	Priority Telecommunications Services
SCIP	Statewide Communication Interoperability Plan
SECC	State Emergency Communications Commission
SIEC	State Interoperability Executive Council
SOP	Standard Operating Procedure

Acronym	Definition
SPOC	Single Point of Contact
SWIC	Statewide Interoperability Coordinator
WPS	Wireless Priority Service