State of Oregon

Statewide Communications Interoperability Plan

August 2024

Developed by the Oregon State Interoperability Executive Council with
Support from the Cybersecurity and Infrastructure Security Agency
Enterprise Information Services, and the Oregon Department of Emergency Management

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

Greetings,

I am pleased to present the 2024 Oregon Statewide Communication Interoperability Plan (SCIP). This represents Oregon's continued commitment to improving emergency communications interoperability and supporting public safety practitioners and emergency managers throughout the state.

This update meets the requirement of the current U.S. Department of Homeland Security grant guidelines and the State Interoperability Executive Council (SIEC)'s mandate under ORS 403.455. Representatives from Oregon's SIEC and its subcommittees collaborated with state-wide partners including public safety, emergency management, cybersecurity, and emergency communications cooperators to update the SCIP framework with actionable, specific and measurable goals and objectives. They also identified champions to help drive progress forward.

Our shared focus is designed to support our state in planning for new technologies and to assist with navigating the ever-changing emergency communications ecosystem. Our goals incorporate lessons observed from recent disasters and critical incidents and seek to ensure the next time we face similar threats, we are better prepared to respond, endure and recover. Our SCIP also incorporates the interoperability improvements identified by the State Interoperability Markers Assessment. This annual assessment allows us the opportunity to reflect on our priorities and ensure we are making intentional, thought-out decisions that align with the state's strategic priorities.

Our updated SCIP comes at a time of great change for interoperable communications within Oregon. A renewed emphasis has been placed on the importance of emergency communications by both national and state governments. Oregon's legislature has seen the need to elevate public safety and emergency management within the state's organizational structure through the creation of two new cabinet level departments. The signing of an interagency agreement recently transferred the Statewide Interoperability Program from the Department of Administrative Services' Office of Enterprise Information Services to the Oregon Department of Emergency Management.

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 everyone in Oregon. With help from public safety and emergency management practitioners, emergency communications cooperators, and our private sector partners, we will work to achieve the goals set forth in this SCIP and achieve our shared vision of "***Seamless interoperable, and resilient emergency communications***."

Sincerely,

William Chapman, ENP
Statewide Interoperability Coordinator (SWIC)
Oregon Department of Emergency Management

INTRODUCTION

The SCIP is a two-to-four-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.
- **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 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 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 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]

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.

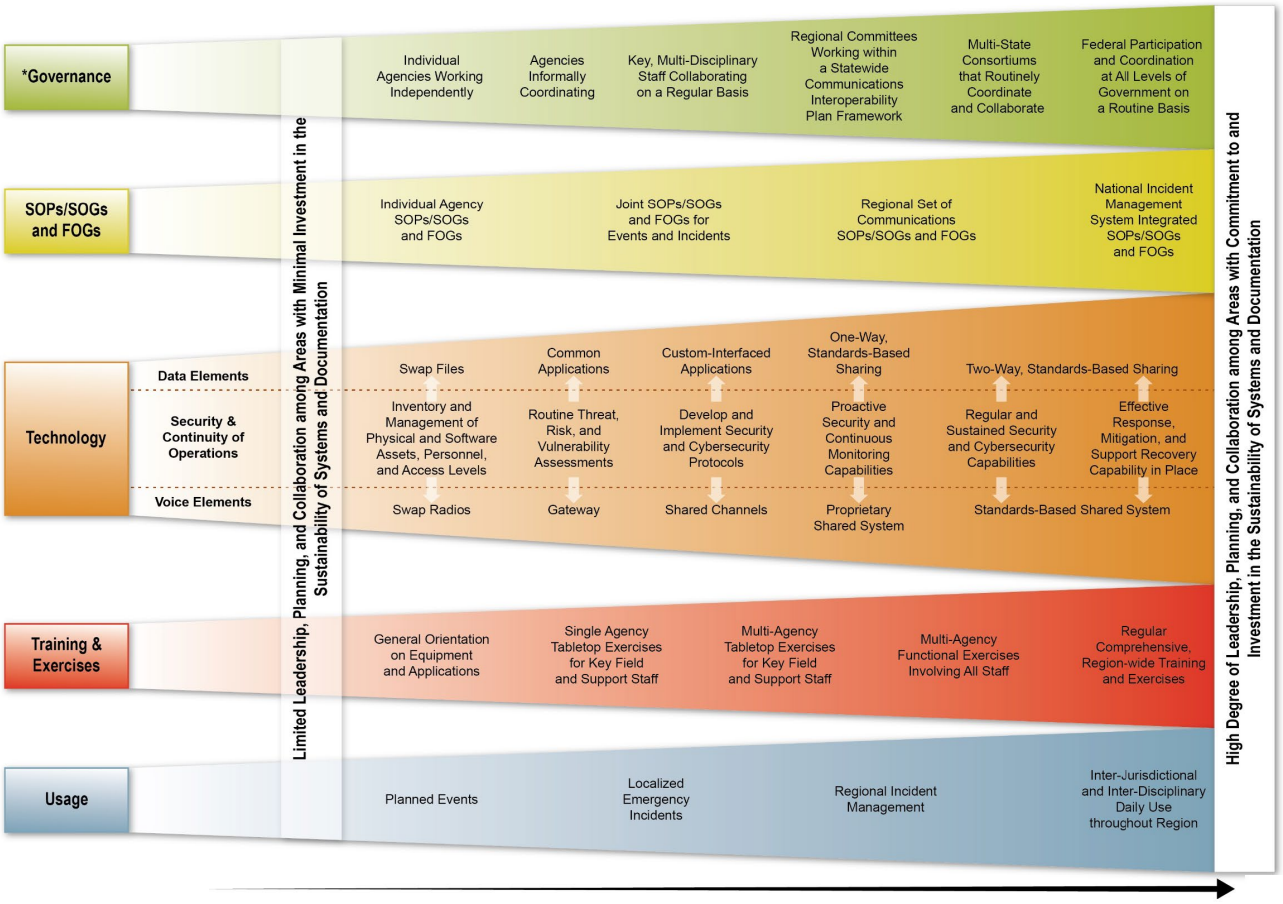


Figure 1: Interoperability Continuum

Interoperability and Emergency Communications Overview

Interoperability is the ability of emergency response agencies to talk to one another via communication systems—to exchange voice and/or data with one another on demand, in real time, when needed, and as authorized.[3] 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.

[1] 2019 National Emergency Communications Plan
[2] Interoperability Continuum Brochure
[3] Wireless Communications Interoperability Awareness Guide

Emergency responders—public safety, and as necessary public services and Non-Governmental Organizations (NGO)—need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Many people assume that emergency response agencies across the Nation already have interoperable communications. However, emergency responders cannot talk to some parts of their own agencies—let alone communicate with agencies in neighboring cities, counties, or states.

Developed with practitioner input from the Cybersecurity and Infrastructure Security Agency's (CISA) SAFECOM program, the SAFECOM Interoperability Continuum is designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications. This tool identifies five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures (SOPs)/standard operating guidelines (SOGs) and field operations guides (FOGs), technology, training and exercises, and usage of interoperable communications. Jurisdictions across the Nation can use the Interoperability Continuum to track progress in strengthening interoperable communications.[4]

Traditional voice capabilities, such as land mobile radio (LMR) and landline 911 services have long been and continue to be critical tools for communications. Advancement of internet protocol-based technologies in public safety have increased the type and amount of information responders receive, the types of tools they communicate with have changed, and the complexity of new and interdependent systems continues to rise. Emerging technologies increase the need for coordination across public safety disciplines, communications functions, and levels of government, as well as with the private sector to ensure emergency communications capabilities are interoperable, reliable, resilient, and secure.

VISION AND MISSION

Vision:

Seamless, interoperable, and resilient emergency communications

Mission:

Provide leadership, strengthen partnerships, and advocate for and investment in voice, data, 911, and public alerts interoperability

GOVERNANCE

The Oregon Revised Statutes (ORS) 403.450 establishes the Oregon State Interoperability Executive Council (SIEC) as Oregon's interoperability governing body. The Council, which is comprised of the Executive, Broadband, Partnership, Strategic Planning, and Technical committees,

[4] SAFECOM Interoperability Continuum

also functions as the Governor's Public Safety Broadband Advisory Group. Other duties of the Council may be found in ORS 403.455 and include:

- Developing standards to promote consistent design and development of public safety communications infrastructures.
- Developing 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.
- Developing recommendations for legislation and for the development of state and local policies that promote public safety communications interoperability in the state.
- Recommending to the Governor, for inclusion in the Governor's budget, investments by the State of Oregon in public safety communications systems.
- Coordinate state, local and as appropriate, tribal and federal activities related to obtaining federal grants for support of interoperability.

The Statewide Interoperability Program (SWI), made up of the Oregon Statewide Interoperability Coordinator (SWIC) and 2 additional full time staff members is responsible for supporting the SIEC and carrying out objectives identified in this plan. The position of the SWIC is also established in ORS and can be found in ORS 403.460. In addition to supporting the SIEC, SWI provides funding and support for the statewide alerts and warnings program known as OR-Alert. OR-Alert is governed by the OR-Alert Governance Committee, a body made up of emergency managers, Public Information Officers (PIOs), Emergency Communications Center (ECC) representatives, and system administrators that collaboratively establishes guidance for use of the system, and for the program.

Oregon Department of Emergency Management

The Oregon Department of Emergency Management (OEM) coordinates and supports statewide emergency services including communications during emergencies and disasters. An interagency agreement transferred the Statewide Interoperability Program and support of the SIEC from the State Chief Information Officer to OEM effective May 1st, 2024. A pending legislative concept is expected to be introduced in the 2025 legislative session to update the underlying statutes to reflect this change. OEM also houses the State's 911 Program which oversees the administration of the appropriation of the state 911 tax and administers the state 911 network. The current 911 tax is set at $1,25/line or device capable of reaching 911 and applies to landlines, postpaid wireless, and voice over internet protocol (VOIP) lines. For prepaid wireless, the tax is applied for each retail transaction. The Program is advised by the Public Safety Answering Point (PSAP) Advisory Committee made up of representatives from around the state. The Program is also engaged in strategic planning to deploy a NG911 network and core services in the coming years. They have formed a NG911 Project Steering Committee to support this project.

Oregon State Police

Presently, the Oregon State Police serves as the state warning point via the Oregon Emergency Response System (OERS). This function will transition to OEM in July of 2025. OSP currently maintains two geographically diverse command centers that also serve as back-up dispatch centers for local law enforcement agencies in the state: the Northern Command Center, housed in Salem;

and the Southern Command Center, housed in Central Point. OSP is also responsible for issuing America's Missing: Broadcast Emergency Response (AMBER) alerts on behalf of the state.

Oregon Department of Transportation

The Oregon Department of Transportation (ODOT) maintains the State Radio System, utilized by both ODOT and Oregon State Police (OSP). ODOT is also responsible for operating the ODOT Transportation Operations Centers, acting as dispatch hubs, in Portland, Salem, Bend, and Central Point, and maintaining the ODOT Intelligent Transportation System communication devices. ODOT is also responsible for maintaining all dispatch consoles for both ODOT and OSP.

Oregon Department of Corrections

The Oregon Department of Corrections (ODOC) radio system serves all the institutions in the department by providing communication services to staff as a component of institution security and safety. The equipment used by staff includes consoles for command and control in control centers; handheld portables radio for use while inside and on the grounds of the institutions; and mobile radios for use outside institutions.

The behind-the-scenes radio system infrastructure is configured in a hybrid model, which means some institutions are operating legacy equipment and other institutions are operating modern Association of Public-Safety Communications Officials (APCO) P25 digital systems. Specifically, at the time of this writing (July 2024), Snake River Correctional Institution (SRCI), Two Rivers Correctional Institute (TRCI), Eastern Oregon Correctional Institution (EOCI), Powder River Correctional Facility (PRCF), Columbia River Correctional Institution (CRCI), Centers for Disease Control and Prevention (CDC), Santiam Correctional Institute (SCI) are operating the L3Harris 10.4 equipment; Deer Ridge Correctional Institution (DRCI) is operating legacy L3Harris 10.2 and Coffee Creek Correctional Facility (CCCF) is operating legacy L3Harris 9 equipment. Lastly, Oregon State Police (OSP), Oregon State Correctional Institute (OSCI), South Fork Forest Camp (SFFC), Warner Creek Correctional Facility (WCCF) are operating legacy analog equipment. All the legacy equipment, analog and digital, will be replaced with L3Harris digital equipment with a final upgrade to version 10.7 to complete the transition to the APCO P25 digital systems by the end of 2025.

The infrastructure that supports this radio system is a network of sophisticated server-based repeater systems located at each institution to automatically route voice traffic to its destination – either local or distant. Future enhancements include integration with cellular networks for statewide operation, interoperability with other public safety organizations including emergency management, and improved command and control across the department. This modern radio system is supported by one manager, one project manager and four communication analysts providing central administration, provisioning, and monitoring to ensure the entire ODOC radio system is operational.

Other Agencies

The **Oregon Department of Forestry** (ODF) maintains a conventional analogue radio system throughout the state for use while operating on ODF protected lands. Additionally, they maintain a large cache of communications equipment and vehicles in support of their wildland fire

suppression mission. ODF also operates the Forest Watch Wildfire Detection Camera System which is monitored by ODF Dispatchers in several centers across the state.

The **Oregon Department of State Fire Marshal (OSFM)** maintains communications vehicles and personnel to support their incident management teams involved in all-hazards response, particularly in the wildland urban interface.

The State Chief Information Officer (CIO) leads the Office of **Enterprise Information Services (EIS)**, which oversees cybersecurity and state data center services. EIS maintains oversight over all state information technology projects and supports enterprise IT governance structures. EIS also provides IT modernization services, project management, and technical engineering services in addition to quality assurance services required under state statute. EIS also houses the EGOV program which supports state website infrastructure.

Governance Challenges

Oregon seeks to address on-going challenges including:

- Facilitating communication among county departments and stakeholders during emergencies
- Engaging elected officials and high-ranking personnel
- Addressing personnel shortages
- Funding and resource shortages
- Training for unique events like the Cascadia earthquake
- Enhancing the adaptability and proficiency of internal communication through planning, training, and exercise, amongst an already overtaxed community
- Disseminating accurate information to the public during an emergency
- Promoting interoperability between public and private partnerships
- Navigating the variety of governance models across Oregon

Strategies for overcoming these challenges involve instituting uniform communication plans, aided by the SIEC's collaboration and coordination, spanning various jurisdictions and neighboring states.

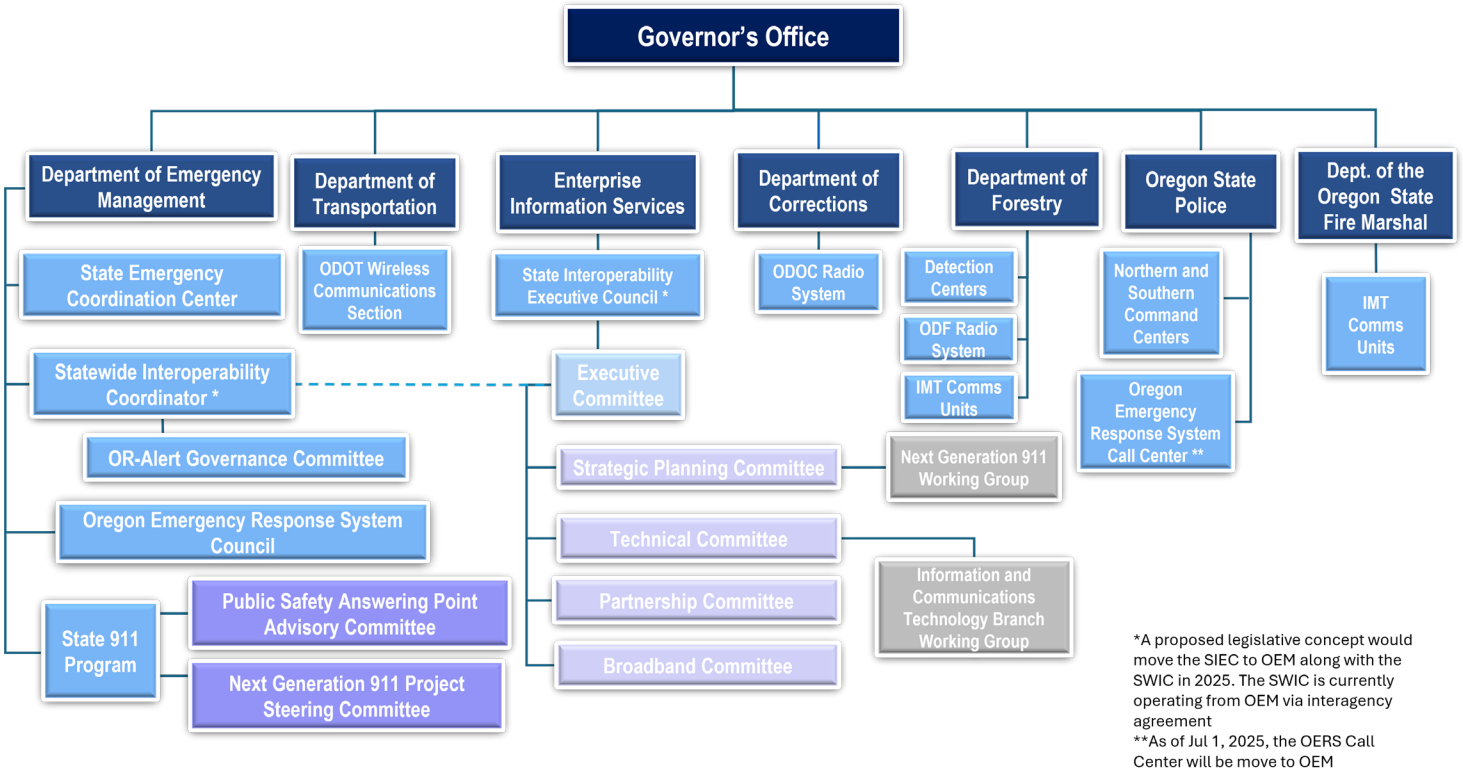
The SIEC has also supported the development of Regional Interoperability Committees (RICs), which has resulted in the development of the Washington-Oregon Regional Interoperability Committee along the Columbia River Gorge. Additional RIC-like groups include the Portland Dispatch Center Consortium (PDCC) and the Emergency Alerts and Warnings Working Group in the Regional Disaster Preparedness Organization of the Portland Urban Area Security Initiative (UASI), the Lane Regional Interoperability Group, and the Linn-Benton Regional Interoperability Group, SWI staff is also working with CISA and local stakeholders to develop a RIC along the southern coastal region of the state.

Involving more citizen volunteers and embracing community-wide planning approaches are an essential building block for comprehensive preparedness. Addressing the diverse set of needs between rural and urban areas, as well as within localities, and among tribal governments, presents opportunities for creative thinking and tailored solutions. Sensitivity to changing local needs and

technologies deployed while updating communications and response plans is essential for effective cooperation.

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

Figure 2: Oregon's Emergency Communications Governance Map



Governance goals and objectives include the following:

Governance	
Goals	**Objectives**
1. Provide effective governance and leadership for the emergency communications ecosystem in Oregon.	1.1 Update Appendix B (Grant Guidance and Investment Priorities) with local input of needs in 2024.
	1.2 Conduct one cross border State Executive Interoperability Council (SIEC) meeting with the State of Washington.
	1.3 Increase Region 10 Regional Emergency Communications Coordination Working Group (RECCWG) meeting attendance to 225 attendees in 2024.
	1.4 Work with Department of Emergency Management (ODEM) and the Public Safety Answering Point (PSAP) Community to evaluate efficiency of Working Groups, and Advisory Bodies related to NG911.
	1.5 Formalize governance ties between Oregon Wildfire Detection Camera Interoperability Committee (OWDCIC) and the SIEC through the inclusion of an SIEC liaison to OWDCIC Leadership.
	1.6 Formally adopt proposed Mission Critical Push-to-Talk (MCPTT) naming conventions for Interoperability talkgroups.
	1.7 Produce a 25 Year report on the activities of the SIEC for delivery to the Governor, Legislature, and other interested parties.
	1.8 Create a catalog of needed policies requiring legislation that promote public safety and emergency communications interoperability in Oregon, including a final outcome report to legislature.
	1.9 Develop and publish SIEC Newsletter editorial process and publishing schedule, including guest article submission and review process.
	1.10 Produce a special edition of the SIEC Newsletter focused on emergency communications cybersecurity.
	1.11 Distribute a signed copy of the 2024 Oregon SCIP to the Governor, Legislative Assembly and State Chief Information Officer.
2. Modernize and strengthen Oregon's emergency communication plans.	2.1 Develop a statewide Continuity of Communications Plan for state agencies, Emergency Operations Centers (EOCs), and PSAPs. Primary, Alternative, Contingency, and Emergency (PACE).
	2.2 Publish Oregon Tactical Interoperable Communications (TIC-FOG).
	2.3 Update State Emergency Support Function (ESF) -2 plan Communications Plans.
	2.4 Update State Communications Unit (COMU) Program to reflect Information and Communications Technology

Goals	Objectives
	Information and Communications Technology (ICT) Branch Functional Guidance
	2.5 Create a strategic plan for the development of a statewide Telecommunicator Emergency Response Taskforce (TERT) program.
	2.6 Conduct a PACE planning workshop for local level agencies.
	2.7 Complete the state AUXCOMM plan.
	2.8 Update OR-Alert Statewide Alerts and Warnings Guidance.
3. Develop and deliver training, exercises, with evaluation programs enhancing knowledge and targeting gaps across all emergency communications technologies.	3.1 Conduct gateway training for members of the Information and Communications Technology (ICT) Branch.
	3.2 Develop framework that enables new Information and Communications Technology Branch personnel to shadow experienced personnel during real world events/incidents.
	3.3 Develop a repository for institutional knowledge/information sharing to be shared with new information and communications technology branch personnel.
	3.4 Identify and develop state-certified Information and Communications Technology Information and Communications Technology (ICT) instructors to deliver training by March 2025.
	3.5 Hold one statewide full-scale communications exercise with opportunities for Personnel Task Book (PTB) sign offs.
	3.6 Hold one statewide tabletop exercise focused on emergency communications.
	3.7 Conduct CASM power user (Bootcamp) training.
	3.8 Conduct one statewide OR-Alert Exercise.
	3.9 Train 45 new Information and Communications Technology (ICT) Branch Members.
	3.10 Develop Exercise in a Box Program to support Emergency Communications.

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

Public Safety Land Mobile Radio (LMR) in Oregon

As a home rule state, Oregon's Public Service Agencies each are responsible for their own radio communications; there is no single statewide public safety radio system as in other states. As a result of this governance style, interoperability is accomplished through the "system of systems" model, where multiple jurisdictions maintain separate radio system networks ("cores") but focus on interconnections and cooperation with neighboring areas to ensure regional coverage. This operational concept includes a mix of:

- **Trunked Radio Systems** (TRS) that cover the more densely populated areas of the state such as the Willamette Valley, the Portland Metropolitan Area, Central Oregon, and portions of the Columbia River Gorge. These systems feature wide-area coverage, resilient network design, and many feature the ability to communicate on other radio systems in the region using network links. These systems generally operate in the UHF portion of the radio spectrum.
- **Very High Frequency (VHF)** radio systems are in heavy use in the more sparsely populated areas of the state, including large swaths of eastern and coastal Oregon. VHF radio systems tend to perform better, with fewer towers required, where there is significant terrain (hills and valleys). VHF systems have been in use for many years, are well known and well understood, relatively simple to implement, and can be built in a variety of ways (single site, multiple sites with voting, simulcast, and multicast).

Interoperability between these two general types of LMR is generally accomplished through one or more methods, including:

- Radio sharing between agencies, i.e. monitoring two or more radios on two or more frequencies
- Direct patches between talk groups or frequencies at the radio network level
- Console patches as needed/on demand through PSAPs and dispatch centers
- Network-level interconnections using techniques like ISSI that allow roaming between radio networks and for talk groups and talk paths that span multiple networks

State Radio System

The Oregon Department of Transportation (ODOT) state radio system serves as the foundation for statewide interoperable radio communications by providing communications for ODOT and OSP along with other state agencies. The ODOT system connects directly to several large local trunked radio systems via Inter-RF Subsystem Interface (ISSI) links. These links allow for the use of shared talk groups between regions and agencies, as well as in some cases (when both agencies agree) the ability for first responders to “active roam” onto another agency’s radio system, in a fashion very similar to cell phone roaming. Currently, the ODOT system is a P25 Phase 2 system consisting of 49 radio sites and features interconnections to:

- The SW7, Washington/Clackamas/Newberg (WCN), and Umatilla Morrow Radio & Data District (UMRDD) radio systems via ISSI links
- The Portland 800 system via patches in the WCN network
- A mix of console and over-the-air patches that connect local agencies on conventional radio systems

The Deschutes County 911 Service District has a partnership with ODOT on the Statewide P25 radio system. Deschutes County 911 maintains twelve P25 radio sites that are attached to the ODOT Statewide P25 radio system core. Those 12 sites with the addition of 10 ODOT radio sites (for a total of 22 sites) provides radio coverage in the Central Oregon area. The combined system is primarily utilized by the nine fire agencies and five police agencies that provide local public safety

services along with numerous general government service agencies and regional mutual aid collaborators.

Challenges Facing LMR

- The VHF spectrum has become extremely congested, with more users requiring space than there are available frequencies for use. This fact can make expansions or updates of existing radio systems to replace obsolete equipment or serve additional users over larger areas difficult
- The funding model for LMR systems varies widely across the state, with some systems charging users annual per-radio or per-connection fees to cover costs, while others treat the radio system as a core business function. In many jurisdictions, the cost to replace or upgrade subscriber units or the system itself is much higher than available funding or revenue
- The high cost of modern radios (several thousands of dollars per unit) is a challenge for many smaller jurisdictions, who lack the tax base and/or resources to acquire sufficient equipment
- Redundancy and resilience are a challenge, especially in more rural areas dependent on a single system or single tower to provide services over a wide area
- A modern trunked radio system depends on access to electrical power, links to communications backhaul networks (microwave, fiber, cable, or copper wire telephony), and a host of computer systems to provide service. There are numerous risks to these systems, including physical disruption, environmental effects such as wildfires, and electronic attacks (cyber threats) including intentional interference, ransomware/malware, denial-of-service (DOS) attacks, and unauthorized system access by bad actors

Opportunities for LMR

- The increasing use of Long-Term Evolution (LTE) cellular devices alongside gateway and network technologies bring the possibility of efficient fusion of cellular and LMR technologies to expand coverage at lower cost
- The advent of (relatively) fast and cost-efficient low earth orbiting satellite systems for voice and data offer another potential source of alternate backhaul for remote radio sites where microwave relay is currently the only connectivity available
- LMR continues to be an easily accessible, affordable, and highly reliable communications method for public safety that tried, tested, and well-known by nearly all first responders.
- Additional short-term interoperability gains in Oregon's LMR environment rely mostly on policies, procedures, and coordination rather than new hardware purchases, making continued investment in LMR systems cost-effective for State agencies and local governments

911

Current 911 systems nationwide were developed using 1960s technology and were designed to handle wired landline calls on analog telephone systems. These legacy systems have served their purpose for the last five decades; however, communications technologies that are used to call 911 have changed dramatically over the last 15 years and continue to change rapidly. As the advancement and ease of access to new technologies expand, traditional wired home telephone continues to be replaced by wireless cellular and VoIP phones. Similarly, the volume of 911 calls from wireless and VoIP phones has grown exponentially, with over 80% of emergency calls in Oregon being made from a wireless cellular device in 2022. To support the delivery of these non-wireline 911 calls an overlay was developed to leverage delivering over the existing analog system. This augmented system became known as the Enhanced 911 (E911) system.

While the system design has evolved to support advances in communications technology, it has not been an easy evolution, nor does it fully support the communications services citizens of the state currently use. These evolutions include advanced application integration of supplemental device-based hybrid location information service known as RapidSOS, updating the frame relay to a Multi-Protocol Label Switching (MPLS) network, and over-the-top text messaging overlays, for the State. The secure deployment of RapidSOS supported the delivery of improved location data to PSAPs through a foundational Emergency Services IP Network (ESInet).

Despite these continued evolutions, the existing system is not able to keep up with the continued technological advances and reliance on wireless and data-based communications across the nation. Recognizing the limitations of the current E911 system, the National Emergency Number Association (NENA) initiated a project to define the Next Generation of 911 (NG911). NG911 will allow 911 requests from multiple devices and technologies, and provide a new mission critical, redundant yet flexible system to serve 911 now and into the future. The central theme of NG911 is a digital network that will allow PSAPs to receive text, video, photos and data, in addition to voice. This national effort was initiated over ten years ago and has resulted in a new, open standard, utilizing today's state-of-the-art technologies and became known as NENA STA- 010.2-2016, or "i3" Version 2 for short. Several states are already in the process of migrating from their legacy E911 system to an NG911 system based on the current NENA standard.

To date, the Oregon Department of Emergency Management in partnership with Oregon's Public Safety Answering Points, statewide communications and statewide technology stakeholders have partnered in the development of a strategic plan for achieving an NG911 ready state. The department is currently in the process of finalizing a business case for the acquisition of a fully vendor managed NG911 solution with early estimated deployment beginning within 2025. In addition, considerable efforts and progress has been made in the preparation of statewide Geographic Information Systems (GIS) data in support of the NENA standard and is the centerpiece of a fully functional NG911 service.

In addition to these efforts, the Department, in 2023 began a project to replace the existing internet protocol (IP) network interconnecting all 43 statewide PSAPs. This network provides the transport of Automatic Location Information (ALI) data provided to assist the PSAP with locating callers, vendor managed services access to install and maintain critical software/security patches, and the transport of supplemental caller location data provided through RapidSOS vendor provided services. Within the scope of this network replacement, increasing network provider diversity was deemed critically necessary to improve network uptime and service availability. As of June 2024,

over fifty percent of the state has migrated to the new network services with a planned completion by the end of the calendar year.

Additional information including timelines and project related progress can be found on the Oregon Department of Emergency Management's NG911 Information Hub Website using the following URL: Oregon NG911 Information Hub.

Technology continues to evolve amongst Oregon's 43 centers, and in 2024, the Statewide Interoperability Program undertook the PSAP Technology Survey, the results of which are below.

911 staffing continues to be challenging in the post-pandemic environment and some centers have turned to technology to enhance the efficiency of call takers including using artificial intelligence to screen non-emergency calls. On the other hand, new technologies including sensors, telematics, and wearables have placed greater demand on emergency communications centers to process data into actionable, usable information that can be communicated to first responders in a timely manner. Nevertheless, the core mission of 911 remains the same: to receive emergency related information from those in distress, and to notify field responders of the emergency.

In 2024, the state undertook an effort to assess the changes taking place in the use of technologies by PSAPs across the state starting in 2020. While results are still be assessed, initial findings indicate that at least 11 PSAPs have upgraded both phone and radio systems in the last four years, and more than 18 centers had made upgrades to their Computer-Aided Design (CAD) system. These rapid changes suggest there are ample opportunities to recognize cost efficiencies and improve interoperability between centers through cooperative procurements and collaboration. More data analysis needs to be undertaken, but the state will also be looking into how it can support technologies in use by the PSAPs from a cybersecurity perspective.

Broadband

In January 2018, Oregon Governor Kate Brown announced Oregon chose to opt into FirstNet to deliver a wireless broadband network to the State's public safety community. Oregon's size, population varying densities and terrain make it a manageable and productive proving ground for refining FirstNet's design and process.

The FirstNet in Oregon Technical Planning Report was created to provide stakeholders with a common understanding of the Nationwide Public Safety Broadband Network (NPSBN). It also prepares them for making decisions regarding technology, network plans and future applications. The report describes FirstNet background, uses and applications, network architecture, governance, stakeholder outreach, the consultation and design process, financial considerations, risks, recommendations, and next steps.

The broadband committee and the SIEC worked through lengthy negotiations and in conjunction with FirstNet, developed the state plan to deploy band 14 capability in the state of Oregon. The plan was accepted, and a 5-year RAN build out effort started in March 2018 and continued through March of 2023.

Alerts and Warnings

OERS

The Oregon Emergency Response System (OERS) Communications Center is the official means of notifying the state of an incident or emergency and serves as the "state warning point" for Oregon. A collaboration between the Oregon State Police and the Department of Emergency Management, OERS is responsible receiving notices related to emergencies, hazardous materials events, threats to the state, and other urgent information, and making notifications to other state agencies and responsible parties. The OERS Call Taking function will transition from OSP to OEM on July 1st, 2025, as part of the ongoing expansion of OEM. As part of this transition, OERS will undergo a transformation to a achieve a vision of a 24/7 Operational Watch Center capability within the state. Staff in the center will not only receive information from callers but will actively monitor new sources of data and analyze threats to the state to better activate and inform a statewide response. For the first time, the state will have a 24/7 critical communications and informational sharing center capable of connecting state, local, federal, tribal, and private response agencies together so they can collaborate, share information, and help people in Oregon on their worst days.

OR-Alert

OR-Alert is Oregon's statewide alerts, warnings, and notifications program. Currently built on the Everbridge program, OR-Alert's mission is to ensure people in Oregon have access to meaningful information to make lifesaving decisions in the face of emergencies. Authorized by the 2020 Legislative Emergency Board, OR-Alert, enables real-time distribution of hazard information in 35 out of 36 of Oregon's counties and tribal governments. This technology also allows county emergency managers to access notification tools including the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS), which can issue wireless emergency alerts to most cell phones in a geographic area and activating the emergency alert system (EAS) across broadcast television and radio. In addition to IPAWS, OR-Alert supports opt-in notifications via SMS text, voice call, email, push notifications via a mobile app, as well as a reverse-911 like capability, posting of messages to high traffic capable website bulletin boards, automatic translation services, automated smart weather alerts, zip code-based alerting, and the ability to pre-script templates for later use.

Alerts are sent by official public safety and emergency management authorities at the local, county, tribal, and/or state level depending on the scope and scale of the emergency. In addition to public alerting, the system is used by many state agencies and local governments for internal messaging including continuity of operations. OR-Alert is built on the Everbridge platform and is in use by 35 Oregon counties, 22 state agencies, and 5 tribal governments. OR-Alert is supported by the Statewide Interoperability Program and funded by the state of Oregon for all participating organizations. The program is governed by the OR-Alert Governance Committee, a collaborative group made up of system administrators, emergency managers, public information officers, emergency communications center representatives, language access coordinators, and others interested in alerts and warnings. The OR-Alert Subcommittee for Recommendations on Alerting Practices in responsible for statewide template development and for recommending changes to the OR-Alert Statewide Alerts and Warnings Guidance which was first published in 2022.

As of July of 2024, there are currently 591,749 total Opt-In contacts within OR-Alert and 4,754,536 total contacts in the system.

ShakeAlert

The ShakeAlert® Earthquake Early Warning (EEW) System is managed by the U.S. Geological Survey in partnership with state agencies and universities including the State of Oregon and the University of Oregon. It is a public safety tool for over 50 million residents and visitors in Oregon, Washington, and California. The ShakeAlert System uses a dense sensor network to rapidly detect earthquakes and United States Geological Survey (USGS) Licensed Technical Partners deliver alerts to people and systems about the potential arrival of strong ground motions. Since March 11, 2021, all Oregonians have been able to receive automated alerts on their mobile phones from several alert delivery providers; FEMA's Wireless Emergency Alert (WEA) system, Google Android operating system, and ShakeAlert-powered applications. To ensure alert delivery, Oregonians should turn on emergency alerts in their phone settings (iPhone users should also enable local awareness). In Oregon, USGS Licensed Technical Partners integrate ShakeAlert data into OR-Alert and other community lifelines and critical infrastructure. Alerts are only delivered for earthquakes that are large enough to be felt and potentially cause damage, with the minimum threshold for WEA alerts being a magnitude 5.0 earthquake with a local shaking intensity of Modified Mercalli Intensity scale IV. The University of Oregon is a cooperative operator of the Pacific Northwest Seismic Network, whose mission includes installing, maintaining, and operating Oregon's sensor and telecommunications network that enables earthquake early detection and alerting in Oregon. ODOT's Wireless Communications Section system and AT&T FirstNet are examples of significant telecommunications partners for the ShakeAlert System in Oregon.

ShakeAlert is also integrated with OR-Alert for situational awareness amongst the emergency management community.

NAWAS

The federal government maintains the National Alert and Warning System (NAWAS) to provide warnings and information dissemination nationwide to designated warning points. Within Oregon there are 40 points. Once a message is received, it is then disseminated across the Oregon State Warning System. While the NAWAS system has been degrading over the last several years, it was recently announced that NAWAS 2.0 is in the works and will be deployed by 2026. The Oregon Department of Emergency Management will continue to work closely with FEMA and AT&T, the NAWAS contractor to support NAWAS and the deployment of NAWAS 2.0 throughout the state.

Cybersecurity

Governor Kate Brown's Executive Order 16-13, "Unifying Cyber Security in Oregon" (EO 16-13) and SB 90 (2017) represent a fundamental shift in how the State of Oregon approaches IT security. The

Enterprise Information Services Cyber Security Services (CSS) division is responsible for enterprise security policy, security monitoring of the State network, enterprise incident response, and enterprise security architecture, as well as dissemination of security training, policy, and best practices across state government. The division is led by a State Chief Information Security Officer (CISO) under the State CIO.

While all agencies are collectively responsible to implement cyber security recommendation provided by the state CISO's office to secure information assets, CSS teams direct, support and implement full cyber security suite of services to increases the collective security posture and resilience of state agencies. Furthermore, through collaboration work with our local government partners to improve cyber resiliency statewide. Moving forward, CSS is focused on the seamless integration of best of breed information security tools, solutions, and personnel into a coordinated multi-sector approach that increases the proactive defensive posture and recognizes cybersecurity as a public good.

Lessons learned from incidents gives strength, data, and capability for assessing areas of improvement. There is a strong situational awareness of cyber attacks that has impacted our local governments and educational institutions across the state, to that effect a collective statewide cyber security plan has been developed to support grant and other related funding opportunities to mitigate assessed cybersecurity gaps. Additionally, work started towards establishing a centralized cyber command within CSS to help with organized response to incidents as a result of ESF 17 activations.

Emerging Technologies

Oregon's Statewide Fire Camera System of Systems

Oregon's Fire Camera System of Systems currently consists of 141 fully operational sites on three unique camera platforms, with forty+ additional sites planned over the next few years. The primary utilization of the statewide system is for early smoke detection. Other use cases include real-time situational awareness for fire managers and first responders, weather monitoring, infrastructure security, smoke monitoring, investigation, and cost recovery. Many camera sites include seismic and other scientific equipment. Camera imagery is available to various emergency management and public safety entities, and in some cases, to the general public.

The University of Oregon and ODF co-chair the Oregon Wildfire Detection Camera Interoperability Committee (OWDCIC), a regional interagency workgroup whose vision is to develop the most integrated, and interorganizational wildfire detection system in the United States that provides immediate statewide access for the most efficient and effective emergency response, thereby ensuring the quality of life and protection of resources in Oregon. The mission of the OWDCIC is to build relationships, increase wildfire detection camera interoperability and resilience, ensure cross jurisdictional/cross-governmental communications and cooperation, and identify and implement best practices across the all-risk emergency operations ecosystem. Three focus areas are:

Policy

- Develop policy consistency between platforms - consistent system data points, analytics, and reporting between platforms
- Develop and publish a common reference library of documents and maps – present on a shared interactive web service
- Define current and expand potential use cases of the system

Technology

- Site installations focused on shared planning, implementation, deployment, maintenance, and sustainability
- Identify, access, and implement new technologies
- Create robust, shared communications hubs for efficient data backhaul
- Pilot and establish interoperability between systems where it is feasible
- Ensure system solutions tie directly to response
- Increase cyber resilience of camera data networks and systems including implementation of cybersecurity measures identified through the development of a system assessment or cybersecurity plan

Funding

- Explore direct, complimentary, and other diverse funding sources to develop, implement and maintain the legacy camera systems and continued maintenance of the statewide camera system via grant funding and other fund sources through SIEC channels

Mission Critical Push-to-Talk

Like other states, Oregon public safety has been somewhat slow to adopt mission critical push-to-talk and generally does not view it as a direct replacement for LMR. Deployments have been somewhat limited to support and command personnel away from the frontline, or for situational awareness while responders are away from their home jurisdiction. One barrier to adoption remains a lack of ubiquitous coverage of the state by any carrier.

Statewide Interoperability is working with the SIEC and cellular carriers to adopt a standard nomenclature for MCPTT interoperability talkgroup naming for services that meet the 3GPP standard of mission critical push-to-talk in hopes that interoperability across carrier applications between talkgroups will one day be achieved. The program is also working on long range plans to deploy IP gateways as the infrastructure to bridge MCPTT applications between carriers. The proposed standard MCPTT Oregon Interoperability talkgroups are:

1. BF-OR-CALL-50
2. BF-OR-TAC-51
3. BF-OR-TAC-52
4. BF-OR-TAC-53
5. BF-OR-TAC-54
6. BF-OR-MOB-59
7. BF-OR-ECC-60

8. BF-OR-LAW-61
9. BF-OR-FIRE-63
10. BF-OR-MED-65
11. BF-OR-UTIL-88
12. BF-OR-SAR-90
13. BF-OR-EM-92
14. BF-OR-DOT-94
15. BF-OR-EDU-96
16. BF-OR-AG-58

Where:

- BF: indicates a Broadband MCPTT Talkgroup
- OR: Oregon Statewide Use
- CALL: Calling
- TAC: General Public Safety Tactical Use
- MOB: Mobile/Deployable
- ECC: Emergency Communications Centers/PSAPs
- LAW/FIRE/EMS: Discipline Specific Tactical
- UTIL: Utility
- SAR: Search and Rescue
- EM: Emergency Management
- DOT: Transportation
- AG: Air to Ground

Machine Learning/Artificial Intelligence

Public safety in Oregon remains somewhat hesitant to engage with artificial intelligence and machine learning but has taken the initial steps to make use of these technologies to increase the efficiencies of operations. Examples include ECCs deploying systems to triage non-emergency calls, limited deployment of A.I. to monitor camera systems for early detection of wildfires, and use of generative applications to assist with document analysis and content generation. In November of 2023, Governor Kotek issued Executive Order 23-26 directing the creation of the Oregon State Government Artificial Intelligence Advisory Council whose purpose is to recommend how the state should leverage A.I. while honoring the values of transparency, privacy, diversity, equity, and inclusion. The Council shall make recommendations within a year of convening.

First Responders Applications

Based on a preliminary survey undertaken in partnership with the Oregon State Sheriff's Association, it was found that there are more than 70 different mobile applications in use by sheriff's departments across the state. It is believed that combined with other law enforcement agencies, fire, and EMS agencies, this number easily surpasses 100. Applications (apps) are present across disciplines and enable responders to accomplish a wide range of tasks from completing reports to issuing emergency alerts, drawing maps and navigating, to reviewing body camera footage. The number of applications in use present their own interoperability challenges, and more information is needed about how agencies are operationalizing this data in multi-agency environments and overcoming these challenges.

One early success story in this arena has been the Oregon Department of Forestry and Oregon State Fire Marshal's build out of the State of Oregon Fire Situation Analyst (SOFSA) which serves as the statewide common operating picture of wildfire incidents and response for both ODF and OSFM. Built on the Intterra platform and accessible via web browser on any device, SOFSA displays a variety of wildland fire and fire service information for statewide situational awareness. SOFSA displays real-time fire intelligence from official federal fire reporting systems such as ICS-209, iROC, IRWIN-aggregated dispatch, mapping and reporting systems like WildCAD, InFORM and NIFC national incident map services. SOFSA also displays key weather, fire environment information and land ownership and reference information that can be viewed for situation assessment and analysis. Key data resources are satellite-based fire detection, lightning and data from large fire Incident Action Plans. There is also a module where infrared imagery and video from ODF Multi-Mission Aircraft can be viewed in real-time, when flight missions are active.

988: A growing, national and statewide network to help callers with mental health crisis

Since the July 2022 transition of the National Suicide Prevention Lifeline to a new three-digit number, 988, Oregon has been developing an expanded, interoperable service for mental health support, crisis response and suicide prevention. 988 connects people 24/7, 365 days a year, to trained crisis counselors via phone, text and chat.

Interoperability is key to 988's impact to ensure that people in crisis get access to the right type of help from the right type of helper. That's why Oregon's 988 call centers, 911 Emergency Communication Centers, and county-run Mobile Crisis Intervention Teams across the state have been collaborating to integrate 988 and crisis response into existing emergency response structures. Additionally, the 988 national network is making technology improvements that will further enhance local interoperability. 988 calls are currently routed by phone number, which means that any calls placed from phone numbers outside of Oregon will route to other states. Starting in September 2024, the 988 national network will begin a transition to georouting, which will improve location-accuracy and connect more 988 callers to local Oregon centers.

Learn more about how 988 and the state's behavioral health crisis system are growing on the Oregon Health Authority website.

Technology and Cybersecurity	
Goals	**Objectives**
5. Improve Oregon's public safety and emergency communications technology and infrastructure so that it is resilient, efficient, interoperable, and meets the needs of public safety.	5.1 Utilizing results of Regional Resiliency Assessment Program (RRAP) data, create a Resilient Emergency Communications Center Model that can be applied across the state.
	5.2 Provide translations for OR-Alert SCRAP Templates into 3 additional languages.
	5.3 Based on nationwide guidance, adopt a standard definition of the public safety communications ecosystem to promote data interoperability between Emergency Communication Centers (ECC's) and field responders.
	5.4 Develop Priority Programming Guide for Interoperability statewide.

Goals	Objectives
	5.5 Deploy Next Generation (NG) ready statewide ESINet to all 43 Primary Emergency Communications Centers, 2 OSP Command Centers, DPSST, and the State Watch Center.
	5.6 Establish statewide interoperable talk path for emergency management agencies' use.
	5.7 Establish 24/7 Watch Desk/Operation Center as part of OERS within the state.
	5.8 Complete current phase of buildout of planned 250 sites for multi-vendor Wildfire Camera Detection Systems throughout the state.
	5.9 Complete a statewide CAD-to-CAD Interoperability Study.
	5.10 Deploy statewide Critical Event Management Software.
	5.11 Develop a strategy to leverage use of sensor data to better inform response to emergencies and disasters.
	5.12 Produce report on the need for additional coverage by the National Public Safety Broadband Network in Oregon.
	5.13 Create Emergency Communications Hazard Mitigations Best Practices Tool Kit.
	5.14 Host Public Safety Emerging Technologies Forum.
	5.15 Produce educational product on best practices/considerations of low earth orbit satellite technology for incident response.
6. Strengthen Oregon's emergency communications ecosystem cybersecurity posture.	6.1 Host a joint emergency management and cybersecurity awareness professional development event.
	6.1 Host one cybersecurity awareness webinar with a focus on how to collect and catalog public safety communications incidents.
	6.2 Develop a cyber incident response team in support of ESF-17. (Cyber and Infrastructure Security).
	6.3 Create standardized procurement contract language to increase the cybersecurity and resilience of emergency communications systems.

FUNDING

During the 2023-2025 biennium, the Statewide Interoperability Program, including operational support and salaries for the SWIC, and two full-time equivalent (FTE) staff, and administrative support, along with and technical, project, and conference support for the SIEC, and funding for OR-Alert are funded by the Department of Administrative Services through Enterprise Information Services' budget. Currently these funds are generated through the assessment of other state agencies.

A legislative concept and policy option package has been introduced to transfer the Statewide Interoperability Program from DAS to OEM in the 2025-2027 biennium. A key factor in the transition will be to identify a source of stable funding for OR-Alert, the SIEC, and SWI moving forward.

Homeland security grant programs including the Emergency Management Performance Grant, and the State Homeland Security Grant Program have not generally been available to support

interoperability initiatives however the transition of these programs to OEM may enable these as possible sources of funding in the future.

Currently the 911 network is funded by the 911 tax administered by the OEM 911 Program. The tax also funds a portion of operational expenses at individual emergency communications centers. It is estimated that the tax funds approximately 45% of the total operating costs of operating 911 centers across the state on average. No state general funds are utilized. Both ODOT and OSP contribute funding to support the State radio system.

In Oregon, a persistent challenge lies in securing funding for infrastructure upgrades in remote rural regions with unreliable communication networks. Additionally, the expense of new subscriber units, particularly in rural areas, presents a substantial hurdle.

Funding goals and objectives include the following:

Funding	
Goals	**Objectives**
7. **Promote adequate funding for Oregon's public safety and emergency communications systems (including infrastructure, people, training, and equipment).**	7.1 Draft a recommendation to the Governor's office identifying needed investments in the public safety communications ecosystem in Oregon for the 25-27 biennium.
	7.2 Introduce and support a Policy Option Package to support, expand, and sustain funding of LMR deployable assets including Strategic Technology Reserve trailers.
	7.3 Conduct grant applications workshop, including information on how to identify, apply, and manage emergency communications grant opportunities.
	7.4 Develop a catalog of existing and needed statewide contracts necessary to sustain public safety and emergency communications services. Collaborate with DAS Procurement to fill gaps if possible.
	7.5 Develop recommended communications related equipment lists for the SPIRE grant program with stakeholder input and submit to the Homeland Security Council for consideration.

IMPLEMENTATION PLAN

Each goal and its associated objectives have a timeline with a target completion date, and one or multiple owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require the support and cooperation from numerous individuals, groups, or agencies, and will be added as formal agenda items for review during regular governance body meetings. The Cybersecurity and Infrastructure Security Agency's (CISA) Interoperable Communications Technical Assistance Program (ICTAP) has a catalog[5] of technical assistance (TA) available to assist with the implementation of the SCIP. TA requests are to be coordinated through the SWIC.

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

Goals	Objectives	Owners	Completion Dates
1. Provide effective governance and leadership for the emergency communications ecosystem in Oregon.	1.1 Update Appendix B (Grant Guidance and Investment Priorities) with local input of needs in 2024.	SWIC	Dec 2024
	1.2 Conduct one cross border State Executive Interoperability Council (SIEC) meeting with the State of Washington.	OR & WA SWICs	End of 2024
	1.3 Increase Region 10 Regional Emergency Communications Coordination Working Group (RECCWG) meeting attendance to 225 attendees in 2024.	SIEC Partnership Committee	Dec 2024
	1.4 Work with Department of Emergency Management (ODEM) and the Public Safety Answering Point (PSAP) Community to evaluate efficiency of Working Groups, and Advisory Bodies related to NG911.	SIEC's APCO REP	Dec 2024
	1.5 Formalize governance ties between OWDCIC and the SIEC through the inclusion of an SIEC liaison to OWDCIC Leadership.	SIEC Executive Committee	Oct 2024
	1.6 Formally adopt proposed Mission Critical Push-to-Talk (MCPTT) naming conventions for Interoperability talkgroups.	SWIC	Dec 2025
	1.7 Produce a 25 Year report on the activities of the SIEC for delivery to the Governor, Legislature, and other interested parties.	SIEC Executive Committee	Apr 2027
	1.8 Create a catalog of needed policies requiring legislation that promote public safety and emergency communications interoperability in Oregon, including a final outcome report to legislature.	SIEC's Legislative Working Group (To be created)	Mar 2026

[5] Emergency Communications Technical Assistance Planning Guide

Goals	Objectives	Owners	Completion Dates
	1.9 Develop and publish SIEC Newsletter editorial process and publishing schedule, including guest article submission and review process.	SIEC Partnership Committee	Apr 2025
	1.10 Produce a special edition of the SIEC Newsletter focused on emergency communications cybersecurity.	CISO	Sep 2024
	1.11 Distribute a signed copy of the 2024 Oregon SCIP to the Governor, Legislative Assembly and State Chief Information Officer.	Chair of SIEC	Sep 2024
2. Modernize and strengthen Oregon's emergency communication plans.	2.1 Develop a statewide Continuity of Communications Plan for state agencies, Emergency Operations Centers (EOCs), and PSAPs and Primary, Alternative, Contingency, and Emergency (PACE) planning.	SWIC	Jul 2025
	2.2 Publish Oregon Tactical Interoperable Communications (TIC-FOG).	SWIC	Jun 2025
	2.3 Update State Emergency Support Function (ESF) -2 Communications Plans.	State ESF-2 Lead and Supporting Agencies with support of OEM	Dec 2024
	2.4 Update State Communications Unit (COMU) Program to reflect Information and Communications Technology (Information and Communications Technology (ICT) Branch Functional Guidance.	SWIC	Aug 2024
	2.5 Create a strategic plan for the development of a statewide Telecommunicator Emergency Response Taskforce (TERT) program.	TERT Coordinator	Dec 2026
	2.6 Conduct a PACE planning workshop for local level agencies.	SIEC Technical Committee	Oct 2024
	2.7 Complete the state AUXCOMM plan.	OEM	Dec 2024
	2.8 Update OR-Alert Statewide Alerts and Warnings Guidance.	OR-Alert Governance Committee	Dec 2024
3. Develop and deliver training, exercises, with evaluation programs enhancing knowledge and targeting gaps across all emergency communications technologies.	3.1 Conduct gateway training for members of the Information and Communications Technology (ICT) Branch.	SWIC	TBD
	3.2 Develop framework that enables new Information and communications technology branch personnel to shadow experienced personnel during real world events/incidents.	SIEC's ICT Working Group	Dec 2027

Goals	Objectives	Owners	Completion Dates
	3.3 Develop a repository for institutional knowledge/information sharing to be shared with new information and communications technology branch personnel.	SIEC's ICT Working Group	Dec 2026
	3.4 Identify and develop state-certified Information and Communications Technology Information and Communications Technology (ICT) instructors to deliver training by March 2025.	SIEC's ICT Working Group	Mar 2025
	3.5 Hold one statewide full-scale communications exercise with opportunities for Personnel Task Book (PTB) sign offs (task books).	SWIC	Jul 2026
	3.6 Hold one statewide tabletop exercise focused on emergency communications.	SWIC	Dec 2025
	3.7 Conduct CASM power user (Bootcamp) training.	SWIC	TBD
	3.8 Conduct one statewide OR-Alert Exercise.	OR-Alert Governance Committee	Apr 2025
	3.9 Train 45 new Information and Communications Technology (ICT) Branch Members.	SWIC	TBD
	3.10 Develop Exercise in a Box Program to support Emergency Communications.	OEM Exercise Program	TBD
4. Improve coordination of the emergency communications ecosystem in Oregon.	4.1 Proposed: Verify accuracy of 20% of agencies' information within CASM.	SWIC	Dec 2027
	4.2 Develop standardized operating guidelines and best practices for special event planning related to communications.	SWIC	TBD
	4.3 Provide for coordinated use of interoperability channels within Oregon.	SWIC	TBD
	4.4 Define OWDCIC interoperability plan with stakeholder input.	OWDCIC Co-Chairs	Dec 2025
	4.5 Create a calendar of recurring pre-planned events needing communications coordination.	SWIC	Dec 2024
	4.6 Host Oregon interoperability conference, adding cross border and federal partners.	SIEC Partnership Committee	Dec 2025

Goals	Objectives	Owners	Completion Dates
5. Improve Oregon's public safety and emergency communications technology and infrastructure so that it is resilient, efficient, interoperable, and meets the needs of public safety.	5.1 Utilizing results of Regional Resiliency Assessment Program (RRAP) data, create Resilient Emergency Communications Center Model that can be applied across the state.	OEM 911 Program, SWIC	Dec 2025
	5.2 Provide translations for OR-Alert SCRAP Templates into 3 additional languages.	OR-Alert Governance Committee	Dec 2026
	5.3 Based on nationwide guidance, adopt a standard definition of the public safety communications ecosystem to promote data interoperability between Emergency Communication Centers (ECC's) and field responders.	SIEC Technical Committee	Aug 2024
	5.4 Develop Priority Programming Guide for Interoperability statewide.	SIEC Technical Committee	Aug 2025
	5.5 Deploy NG ready statewide ESINet to all 43 Primary Emergency Communications Centers, 2 OSP Command Centers, DPSST, and the State Watch Center.	OEM 911 Program	Dec 2025
	5.6 Establish statewide interoperable talk path for emergency management agencies' use.	OEM	Dec 2027
	5.7 Establish 24/7 Watch Desk/Operation Center as part of OERS within the state.	OEM	Jul 2025
	5.8 Complete current phase of buildout of planned 250 sites for multi-vendor Wildfire Camera Detection Systems throughout the state.	OWDCIC Camera Operators	Jul 2027
	5.9 Complete a statewide CAD-to-CAD Interoperability Study.	SWIC	Dec 2027
	5.10 Deploy statewide Critical Event Management Software.	OEM	Dec 2026
	5.11 Develop a strategy to leverage use of sensor data to better inform response to emergencies and disasters.	SIEC Technical Committee	Dec 2026
	5.12 Produce report on the need for additional coverage by the National Public Safety Broadband Network in Oregon.	SIEC Broadband Committee	Dec 2024
	5.13 Create Emergency Communications Hazard Mitigations Best Practices Tool Kit.	OEM Mitigation Section	TBD
	5.14 Host Public Safety Emerging Technologies Forum.	SIEC Technology and Partnership Committees	Dec 2026

Goals	Objectives	Owners	Completion Dates
	5.15 Produce educational product on best practices/considerations of low earth orbit satellite technology for incident response.	SIEC Technical Committee	Dec 2025
6. Strengthen Oregon's emergency communications ecosystem cybersecurity posture.	6.1 Host a joint emergency management and cybersecurity awareness professional development event.	State Cyber Command Team	Mar 2025
	6.2 Host one cybersecurity awareness webinar with a focus on how to collect and catalog public safety communications incidents.	State Cyber Command Team	Mar 2025
	6.3 Develop a cyber incident response team in support of ESF-17. (Cyber and Infrastructure Security)	State Cyber Command Team	Dec 2024
	6.4 Create standardized procurement contract language to increase the cybersecurity and resilience of emergency communications systems.	SWIC	Dec 2025
7. Promote adequate funding for Oregon's public safety and emergency communications systems (including infrastructure, people, training, and equipment).	7.1 Draft a recommendation to the Governor's office identifying needed investments in the public safety communications ecosystem in Oregon for the 25-27 biennium.	SIEC Executive Committee	Jul 2024
	7.2 Introduce and support a Policy Option Package to support, expand, and sustain funding of LMR deployable assets including Strategic Technology Reserve trailers.	SIEC Executive Committee	Jul 2024
	7.3 Conduct grant applications workshop, including information on how to identify, apply, and manage emergency communications grant opportunities.	OEM Preparedness Section	Dec 2025
	7.4 Develop a catalog of existing and needed statewide contracts necessary to sustain public safety and emergency communications services. Collaborate with DAS Procurement to fill gaps if possible.	SWIC	Dec 2026
	7.5 Develop recommended communications related equipment lists for the SPIRE grant program with stakeholder input and submit to the Homeland Security Council for consideration.	SIEC Technical and Executive Committees	Apr 2025

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 as of 07/31/24.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
1	**State-level governing body established (e.g., SIEC, SIGB).** Governance framework is in place to sustain all emergency communications	Governing body does not exist, or exists and role has not been formalized by legislative or executive actions	Governing body role established through an executive order	Governing body role established through a state law
2	**SIGB/SIEC participation.** Statewide governance body is comprised of members who represent all components of the emergency communications ecosystem.	Initial (1-2) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications	Optimized (5) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 911 ☒ Alerts, Warnings and Notifications
3	**SWIC established.** Full-time SWIC is in place to promote broad and sustained participation in emergency communications.	SWIC does not exist	Full-time SWIC with collateral duties	Full-time SWIC established through executive order or state law
4	**SWIC Duty Percentage.** SWIC spends 100% of time on SWIC-focused job duties	SWIC spends >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 future technology transitions (5G, IoT, UAS, etc.). (Strategic and non-strategic goals are completely different; strategy – path from here to the destination; it is unlike tactics which you can "touch"; cannot "touch" strategy)	<50% are strategic goals in SCIP	>50%<90% are strategic goals in SCIP	>90% are strategic goals in SCIP
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

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
8	**Communications Unit process.** Communications Unit process present in state / territory to facilitate emergency communications capabilities. Check the boxes of which Communications positions are currently covered within your process: ☒ COML ☒ COMT ☒ ITSL ☒ RADO ☒ INCM ☒ INTD ☒ AUXCOM ☒ TERT	No Communications Unit process at present	Communications Unit process planned or designed (but not implemented)	Communications Unit process implemented and active
9	**Interagency communication.** Established and applied interagency communications policies, procedures and guidelines.	Some interoperable communications SOPs/SOGs exist within the area and steps have been taken to institute these interoperability procedures among some agencies	Interoperable communications SOPs/SOGs are formalized and in use by agencies within the area. Despite minor issues, SOPs/SOGs are successfully used during responses and/or exercises	Interoperable communications SOPs/SOGs within the area are formalized and regularly reviewed. Additionally, NIMS procedures are well established among agencies and disciplines. All needed procedures are effectively utilized during responses and/or exercises.
10	**TICP (or equivalent) developed.** Tactical Interoperable Communications Plans (TICPs) established and periodically updated to include all public safety communications systems available	Regional or statewide TICP in place	Statewide or Regional TICP(s) updated within past 2-5 years	Statewide or Regional TICP(s) updated within past 2 years
11	**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	<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

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	channel nomenclature consistency across a state / territory.			
14	**Cybersecurity Assessment Awareness.** Cybersecurity assessment awareness. (Public safety communications networks are defined as covering: LMR, LTE, 911, and A&W)	Public safety communications network owners are aware of cybersecurity assessment availability and value (check yes or no for each option) ☐ LMR ☐ LTE ☐ 911/CAD ☐ A&W	Initial plus, conducted assessment, conducted risk assessment. (Check yes or no for each option) ☒ LMR ☒ LTE ☒ 911/CAD ☒ A&W	Defined plus, Availability of Cyber Incident Response Plan (check yes or no for each option) ☐ LMR ☐ LTE ☐ 911/CAD ☐ A&W
15	**NG911 implementation.** NG911 implementation underway to serve state / territory population.	Working to establish NG911 governance through state/territorial plan. • Developing GIS to be able to support NG911 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • Planning to or have updated PSAP equipment to handle basic NG911 service offerings.	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.
17	**Future Technology/Organizational Learning.** SIEC/SIGB is tracking, evaluating, implementing future technology (checklist)	☐ 5G ☐ Acoustic Signaling ☐ Autonomous Vehicles ☐ Body Cameras ☐ ESInets ☐ GIS ☐ Geolocation	☐ HetNets/Mesh Networks ☐ LMR to LTE Integration ☐ MCPTT Apps ☐ Machine Learning/AI ☐ Public Alerting Software ☐ Sensors ☐ Situational Awareness Apps	☐ Smart Cities ☐ The Next Narrowbanding ☐ UAS (Drones) ☐ UAV (Smart Vehicle) ☐ Wearables ☐ IoT (Cameras)
18	**Communications Exercise objectives.** Specific emergency communications objectives are incorporated into applicable exercises Federal / state / territory-wide	Regular engagement with State Training and Exercise coordinators	Promote addition of emergency communications objectives in state/county/regional level exercises (target Emergency Management community). Including providing tools, templates, etc.	Initial and Defined plus mechanism in place to incorporate and measure communications objectives into state/county/regional level exercises
19	**Trained Communications Unit responders.** Communications Unit personnel are listed in a	<49% of public safety agencies within a state / territory have access to Communications Unit personnel	>50%<74% of public safety agencies within a state / territory have access to Communications Unit personnel	>75%<100% of public safety agencies within a state / territory have access to Communications Unit

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	tracking database (e.g., NQS One Responder, CASM, etc.) and available for assignment/response.	who are listed in a tracking database and available for assignment/response	who are listed in a tracking database and available for assignment/response	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 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
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: ☐ Governance ☐ SOPs/MOUs ☐ Technology ☐ Training/Exercises ☐ Usage	Defined: Documented/established across some lanes of the Continuum: ☐ Governance ☐ SOPs/MOUs ☐ Technology ☐ Training/Exercises ☐ Usage	Optimized: Documented/established across all lanes of the Continuum: ☒ Governance ☒ SOPs/MOUs ☒ Technology ☒ Training/Exercises ☒ Usage

APPENDIX B: ACRONYMS

Acronym	Definition
A&W	Alerts and Warnings
AAR	After-Action Report
ALI	Automatic Location Information
AMBER	America's Missing: Broadcast Emergency Response
APCO	Association of Public-Safety Communications Officials
AUXCOMM/AUXC	Auxiliary Emergency Communications
CAD	Computer-Aided Design
CASM	Communication Assets Survey and Mapping
CCCF	Coffee Creek Correctional Facility
CDC	Centers for Disease Control and Prevention
CIO	State Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
CRCI	Columbia River Correctional Institution
CSS	Cyber Security Services
DHS	Department of Homeland Security
DPSST	Department of Public Safety Standards and Training
DRCI	Deer Ridge Correctional Institution
ECC	Emergency Communications Coordinator
EEW	Earthquake Early Warning
EIS	Enterprise Information Services
EOC	Emergency Operations Center
EOCI	Eastern Oregon Correctional Institution
ESInet	Emergency Services Internal Protocol Network
ESO	Enterprise Security Office
FEMA	Federal Emergency Management Agency
FOG	Field Operations Guide
FTE	Full-Time Equivalent
GIS	Geospatial Information System
HSGP	Homeland Security Grant Program
ICT	Information and Communications Technology
ICTAP	Interoperable Communications Technical Assistance Program
INCM	Incident Communications Center Manager

Acronym	Definition
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
IPAWS	Public Alert and Warning System
ISSI	Inter-RF Subsystem Interface
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MCPTT	Mission Critical Push-to-Talk
MHz	Megahertz
MOU	Memorandum of Understanding
NAWAS	National Alert Warning System
NCSWIC	SAFECOM/National Council of SWICs
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NG911	Next Generation 911
NGO	Non-Governmental Organizations
NPSBN	Nationwide Public Safety Broadband Network
ODEM	Department of Emergency Management
ODF	Oregon Department of Forestry
ODOC	Oregon Department of Corrections
ODOT	Oregon Department of Transportation
OEM	Oregon Department of Emergency Management
OERS	Oregon Emergency Response System
OR-Alert	Oregon-Alert, Oregon's Statewide emergency alerts and warnings system
ORS	Oregon Revised Statutes
OSCI	Oregon State Correctional Institute
OSP	Oregon State Police
OWDCIC	Oregon Wildfire Detection Camera Interoperability Committee
PACE	Primary, Alternative, Contingency, and Emergency
PDCC	Portland Dispatch Center Consortium
PIO	Public Information Officer
PRCF	Powder River Correctional Facility
PSAP	Public Safety Answering Point
PTB	Personnel Task Book
RADO	Radio Operator
RIC	Regional Interoperability Committee
SCI	Santiam Correctional Institute
SCIP	Statewide Communication Interoperability Plan

Acronym	Definition
SFFC	South Fork Forest Camp
SIEC	State Interoperability Executive Council
SOG	Standard Operating Guide
SOP	Standard Operating Procedure
SPIRE	The State Preparedness and Incident Response Equipment
SRCI	Snake River Correctional Institution
SWI	Statewide Interoperability Program
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TERT	Telecommunications Emergency Response Team
TIC-FOG	Telecommunications and Information Systems Field Operations Guide
TICP	Tactical Interoperable Communications Plan
TRCI	Two Rivers Correctional Institute
TRS	Trunked Radio Systems
UASI	Urban Area Security Initiative
UMRDD	Umatilla Morrow Radio & Data District
USGS	United States Geological Survey
VHF	Very High Frequency
VOIP	Voice Over Internet Protocol
WCCF	Warner Creek Correctional Facility
WCN	Washington/Clackamas/Newberg
WCS	Wireless Communications Section
WPS	Wireless Priority Service