State of Oregon

Statewide Communications Interoperability Plan

November 2025

Rev. 3.0

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

Revision Record

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	08/2024	Baseline Document
2.0	03/2025	Added Appendix C: Grant Guidance and Investment Priorities, and Appendix D: National Emergency Communications Plan Priorities.
3.0	11/2025	Interim update. Transition from DAS/EIS to OEM

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

Greetings,

I am honored to present the Oregon Statewide Communication Interoperability Plan (SCIP), Rev 3.0. This document reflects Oregon's unwavering commitment to advancing emergency communications interoperability in service of the public safety practitioners, emergency managers, and communities throughout the state. This revision fulfils the requirements of the U.S. Department of Homeland Security grant guidelines and the State Interoperability Executive Council (SIEC)'s mandate under 403.455

This update comes at a pivotal moment. The 2025 legislative session formally transferred the Statewide Interoperability Program to the Oregon Department of Emergency Management, establishing the Office of the Statewide Interoperability Coordinator as a dedicated, permanent function within OEM. The Office is staffed by a solid team of individuals with vast experience spanning 911 and dispatch, wildland fire, emergency management, radio communications systems and alerts and warnings, a true Dream Team of Statewide Interoperability, positioned to provide sustained leadership and technical expertise in support of the SIEC and the broader emergency communications ecosystem.

Since the 2024 SCIP, Oregon has achieved significant milestones. The Oregon Emergency Response System (OERS) is transitioning to the OERS Watch Center, set to begin operations on July 1, 2026, as a 24/7 Operational Watch Center, the first of its kind in the state's history. Oregon's statewide alerts and warnings program, OR-Alert, continues to grow in reach and capability through increased participation and statewide exercises. Simultaneously, the expansion of Oregon's wildfire detection camera system has advanced significantly, providing early detection and real-time situational awareness to fire managers and first responders.

Interoperability does not stop at state borders. As the Second Vice Chair of the National Council of Statewide Interoperability Coordinators (NCSWIC), I have had the privilege of building partnerships that benefit not only Oregon but the nation. The relationships I established as the SWIC for the State of Washington now extend across the SWIC community nationwide. The collaboration and willingness to share knowledge and resources within this community makes us stronger as individual states and as a nation, and I am committed to leveraging those connections on behalf of Oregon.

Looking ahead, a central theme of this SCIP is confronting the interoperability gaps that exist across Oregon, in both urban and rural communities alike. No community is immune, and the work of the Office of the Statewide Interoperability Coordinator is to bring all communities together to solve these issues. As many of my fellow SWICs across the nation will tell you, most of the time it is not a technology issue. It is about relationships, and it starts with a conversation. Our shared vision remains "Seamless, interoperable, and resilient communications." Let's get to work!

Sincerely,

Jon Lee
Oregon Statewide Interoperability Coordinator (SWIC)
Second Vice Chair, National Council of Statewide Interoperability Coordinators (NCSWIC)
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.

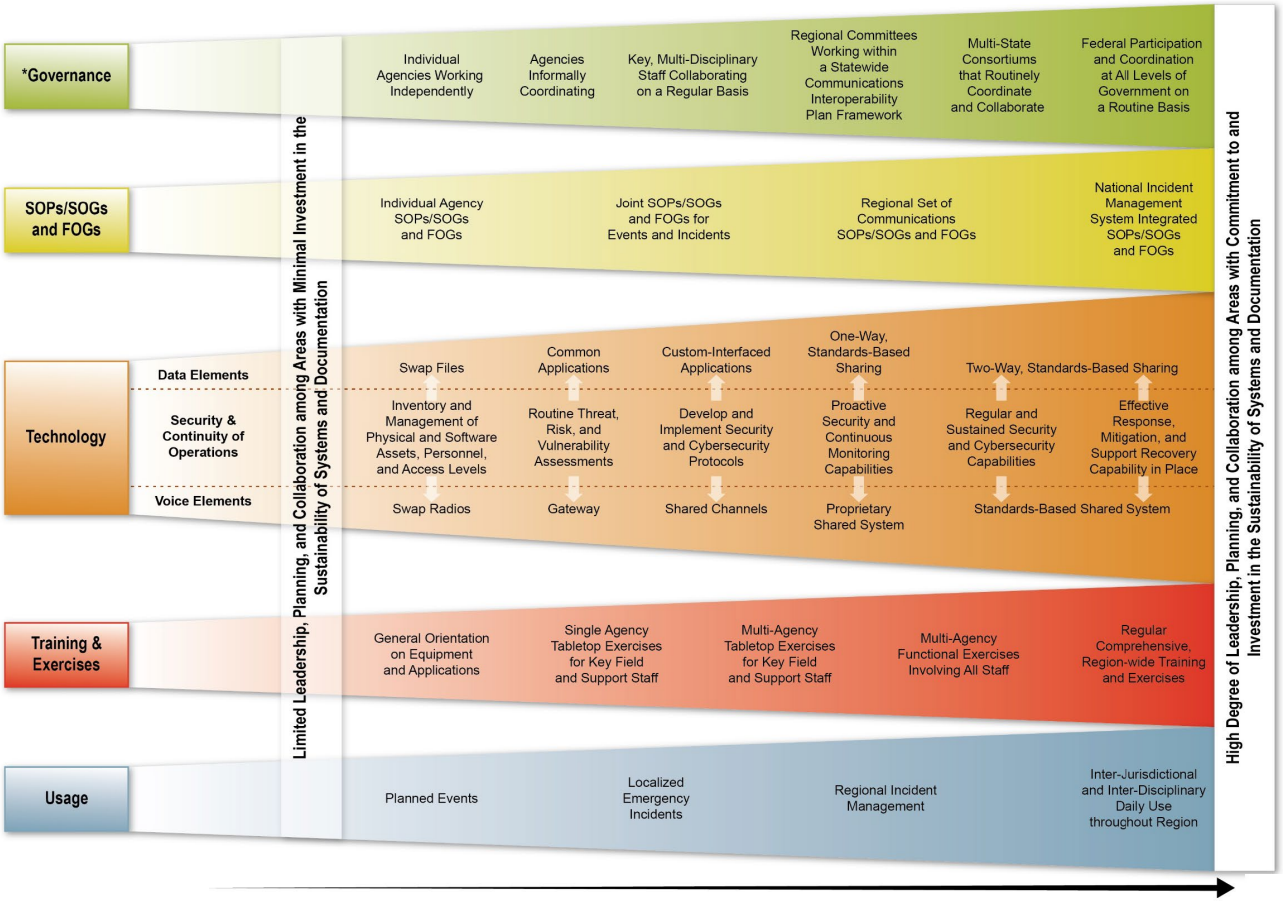


Figure 1: Interoperability Continuum

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,

[1] 2019 National Emergency Communications Plan
[2] Interoperability Continuum Brochure

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.

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

[3] Wireless Communications Interoperability Awareness Guide
[4] SAFECOM Interoperability Continuum

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, 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 Office of the Statewide Interoperability Coordinator, made up of the Oregon Statewide Interoperability Coordinator (SWIC) and 3 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, The Office of the Statewide Interoperability Coordinator 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. The 2025 legislative session under Senate Bill 826, formalized the transfer of the Statewide Interoperability Program from DAS to OEM, creating the Office of the Statewide Interoperability Coordinator as a permanent function within OEM. 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

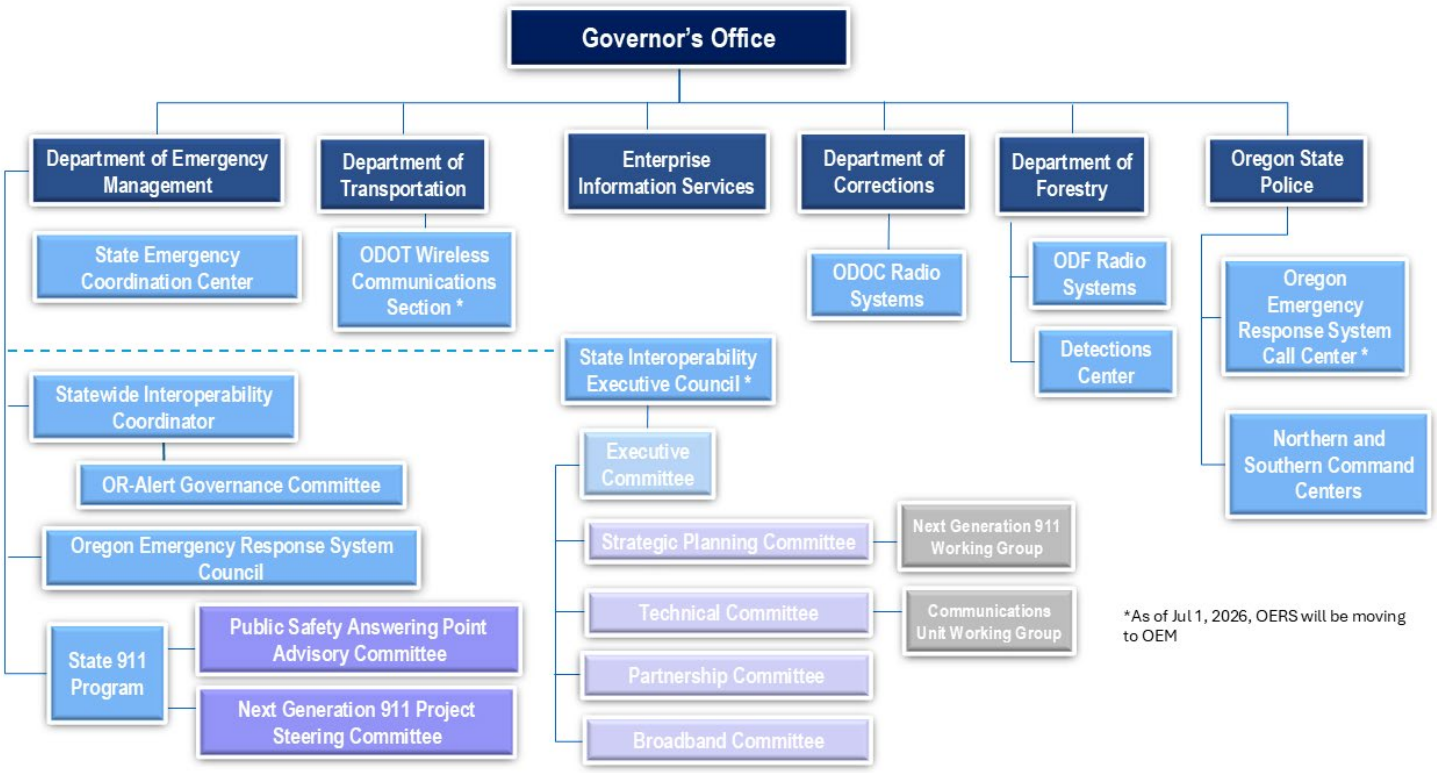
Strategies for overcoming these challenges involve instituting uniform communication plans, aided by the SIEC's collaboration and coordination, spanning various jurisdictions and neighboring states.

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. 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 100 attendees in 2026.
	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 40 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 40 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, 2026, 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 platform, 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 all 36 of Oregon's counties and amongst 5 of Oregon's 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 36 Oregon counties, 27 state agencies, and 5 tribal governments. OR-Alert is supported by the Office of the Statewide Interoperability Coordinator 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.

- OR-CALL-50
- OR-TAC-51
- OR-TAC-52
- OR-TAC-53
- OR-TAC-54
- OR-MOB-59
- OR-ECC-60

- OR-LAW-61
- OR-FIRE-63
- OR-MED-65
- OR-UTIL-88
- OR-SAR-90
- OR-EM-92
- OR-DOT-94
- OR-EDU-96
- OR-AG-58

Where:

- 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

The national standard naming format is as follows:[5]

AA-Type-###-M

This format is broken down as follows:

AA ..... National/State/Tribal/Territorial Designator

The National/State designator is unique two alpha characters to designate the public safety area of operation most commonly used.
US .....National interoperability talkgroup
XX.....United States Postal Service postal code representing U.S. state or territory or TR as a tribal designator

Type ..... Channel Use Designator

The channel use designator is an alphanumeric tag that signifies the primary purpose of operations in the talkgroup. Knowing that APCO is working on the refresh of the LMR naming standard, this document will align type designator for continuity between broadband and LMR naming.

..... Channel Identifier

The Channel Identifier is a numeric two place tag to uniquely identify the specific channel. Channel Identifiers are grouped by national (U.S.), and states/territories/tribes as follows:
X00 – X49..... U.S. (national)
X50 – X99.....U.S. state/territory/tribe
XXX50 – XX99.....Used for state/territory/tribe use when not using predefined types.

M ..... Modifier

The Modifier character is an alphanumeric tag to identify a modification to the default operation type on the resource, when applicable:
D .....Direct mode or talk around use

[5] Standard Talkgroup Nomenclature Framework for Public Safety Broadband

IWF.....Interworking with land mobile radio (LMR) providing supplemental data
ITC.....Interconnected with LMR voice only
DATA .....Data service to include or combine data, voice, images, video, and location based services (LBS)
OFN.....Off network
DPLY .....Deployable supported e.g., Cell on Wings (COW), Compact Rapid Deployables (CRD), Mini-CRD
CCC ..... Cross-carrier communication
VIDEO ..... Video or streaming transmission

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 in 2024, 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.
	5.5 Deploy Next Generation (NG) ready statewide ESINet to all 40 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 Based on the feasibility study, develop a Business Case for a full statewide CAD to CAD solution
	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.

Goals	Objectives
	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.
	5.16 NG9-1-1 Core Services Achieve Stage Gate 3
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[6] 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.

Green cell = Completed, Blue Cell = In Progress, White Cell = Not Started

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	2026
	1.3 Increase Region 10 Regional Emergency Communications Coordination Working Group (RECCWG) meeting attendance to 225 attendees in 2024.	SIEC Partnership Committee	Dec 2026
	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 2026
	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	Feb 2026
	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

[6] Emergency Communications Technical Assistance Planning Guide

Goals	Objectives	Owners	Completion Dates
	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
	1.9 Develop and publish SIEC Newsletter editorial process and publishing schedule, including guest article submission and review process.	SIEC Partnership Committee	Feb 2026
	1.10 Produce a special edition of the SIEC Newsletter focused on emergency communications cybersecurity.	CISO	Aug 2026
	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 2026
	2.2 Publish Oregon Tactical Interoperable Communications (TIC-FOG).	SWIC	Jun 2026
	2.3 Update State Emergency Support Function (ESF) -2 Communications Plans.	State ESF-2 Lead and Supporting Agencies with support of OEM	Jun 2026
	2.4 Update State Communications Unit (COMU) Program to reflect Information and Communications Technology (Information and Communications Technology (ICT) Branch Functional Guidance.	SWIC	Jun 2026
	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	Jun 2025
	2.7 Complete the state AUXCOMM plan.	OEM	Dec 2026
	2.8 Update OR-Alert Statewide Alerts and Warnings Guidance.	OR-Alert Governance Committee	Dec 2026

Goals	Objectives	Owners	Completion Dates
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
	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	TBD
	3.7 Conduct CASM power user (Bootcamp) training.	SWIC	TBD
	3.8 Conduct one statewide OR-Alert Exercise.	OR-Alert Governance Committee	Dec 2026
	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 a plan to support a statewide interoperable TAK environment, including governance, technical architecture, and integration with existing communications and information-sharing systems.	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	Jul 2026

Goals	Objectives	Owners	Completion Dates
	4.5 Create a calendar of recurring pre-planned events needing communications coordination.	SWIC	Dec 2025
	4.6 Host Oregon interoperability conference, adding cross border and federal partners.	SIEC Partnership Committee	Dec 2025
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	Feb 2026
	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	Feb 2026
	5.4 Develop Priority Programming Guide for Interoperability statewide.	SIEC Technical Committee	Aug 2026
	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 2026
	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 2026
	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 Based on the feasibility study, develop a Business Case for a full statewide CAD to CAD solution	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 2026
	5.13 Create Emergency Communications Hazard Mitigations Best Practices Tool Kit.	OEM Mitigation Section	TBD

Goals	Objectives	Owners	Completion Dates
	5.14 Host Public Safety Emerging Technologies Forum.	SIEC Technology and Partnership Committees	Dec 2026
	5.15 Produce educational product on best practices/considerations of low earth orbit satellite technology for incident response.	SIEC Technical Committee	Apr 2026
	5.16 NG911 Core Services to achieve Stage Gate 3	OEM 911	Apr 2026
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	Dec 2026
	6.2 Host one cybersecurity awareness webinar with a focus on how to collect and catalog public safety communications incidents.	State Cyber Command Team	Dec 2026
	6.3 Develop a cyber incident response team in support of ESF-17. (Cyber and Infrastructure Security)	State Cyber Command Team	Dec 2026
	6.4 Create standardized procurement contract language to increase the cybersecurity and resilience of emergency communications systems.	SWIC	Dec2027
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 2026
	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 2026
	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 Emergency Communications Governing Body Established (e.g., SIEC, SIGB):** Governance framework is in place to sustain all emergency communications.	Emergency communications governing body does not exist, or exists but the body has not been formalized by legislative or executive actions.	Emergency communications governing body is established through an executive order	Emergency communications governing body is codified through a state law
2	**Emergency Communications Governing Body Inclusion:** Statewide governance body is comprised of all components of the emergency communications ecosystem (Communication Champion/SWIC, LMR, Broadband/LTE, 911, and AWN) and invites other relevant emergency communications partners to participate in the meetings.	Initial (1-5) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications ☐ Federal components representatives (Count as 1) ☐ CISA (ECC, CSA, etc.) ☐ Federal Law Enforcement ☐ Federal Land Management ☐ Federal Emergency Management Agency ☐ U.S. Department of Health and Human Services ☐ Military, including Coast Guard ☐ State Cyber representatives ☐ State Chief Information Officer ☐ State Legislative Liaison ☐ State Emergency Management Agency ☐ State Homeland Security Advisor or representatives ☐ National Guard ☐ Local or County representatives ☐ Tribal representatives ☐ Other (Please specify)	Defined (6-10) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications ☐ Federal components representatives (Count as 1) ☐ CISA (ECC, CSA, etc.) ☐ Federal Law Enforcement ☐ Federal Land Management ☐ Federal Emergency Management Agency ☐ U.S. Department of Health and Human Services ☐ Military, including Coast Guard ☐ State Cyber representatives ☐ State Chief Information Officer ☐ State Legislative Liaison ☐ State Emergency Management Agency ☐ State Homeland Security Advisor or representatives ☐ National Guard ☐ Local or County representatives ☐ Tribal representatives ☐ Other (Please specify)	Optimized (10+) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 911 ☒ Alerts, Warnings and Notifications ☒ Federal components representatives (Count as 1) ☒ CISA (ECC, CSA, etc.) ☒ Federal Law Enforcement ☐ Federal Land Management ☒ Federal Emergency Management Agency ☐ U.S. Department of Health and Human Services ☒ Military, including Coast Guard ☒ State Cyber representatives ☒ State Chief Information Officer ☒ State Legislative Liaison ☒ State Emergency Management Agency ☒ State Homeland Security Advisor or representatives ☒ National Guard ☒ Local or County representatives ☒ Tribal representatives ☒ Other (Please specify) *Also includes private sector, broadcasters, public safety associations

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
3	**SWIC Position Established**: A full-time employee, either a SWIC or an employee that performs the duties of a SWIC, is in place to promote the performance of all Interoperability Markers emergency communications.	A SWIC position or an employee performing the duties of the SWIC position does not exist	A full-time SWIC position with collateral duties or a full-time employee with the duties of the SWIC position as part of their collateral duties. Also, the SWIC position appears in the Administrative Rule of the state/territory agency that the SWIC serves in or is established through Executive Order.	Full-time SWIC established through executive order or state law
4	**SWIC Office established:** The SWIC has a dedicated office, that includes a deputy SWIC and support staff	A SWIC, or full-time employee performing the duties of a SWIC as collateral duties, is the only person in place to promote the performance of all Interoperability Markers	A SWIC and deputy SWIC are the only two people in place to promote the performance of all Interoperability Markers	A SWIC has a deputy SWIC as well as one or more additional full-time employee/s in place to promote the performance of all Interoperability Markers
5	**SWIC and/or SWIC Office State/Territory Level Coordination:** A state/territory coordination across all emergency communications technologies is at the core of successful emergency communications interoperability. If the SWIC and/or SWIC office is not the primary lead for a specific governance, policy, technology, training & exercise, or usage role, the SWIC and/or SWIC office should play a significant coordinating role in bringing the responsible leads together to further enhance a state or territory ability to improve interoperable emergency communications.	The SWIC and/or its office has coordinated with 1-4 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state/territory level (check all that apply) ☐ 911 – Telephone, CAD, and NG911 ☐ Governance ☐ Training and Exercises ☐ Cybersecurity ☐ Radio Communications Systems ☐ Broadband and Data Systems ☐ Alerts and Warnings ☐ State-level Emergency Management Agency ☐ Priority Telecommunications Services ☐ UASI Involvement ☐ Tribal Engagement ☐ IMT Coordinator	The SWIC and/or its office has coordinated with 1-4 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state/territory level (check all that apply) ☐ 911 – Telephone, CAD, and NG911 ☐ Governance ☐ Training and Exercises ☐ Cybersecurity ☐ Radio Communications Systems ☐ Broadband and Data Systems ☐ Alerts and Warnings ☐ State-level Emergency Management Agency ☐ Priority Telecommunications Services ☐ UASI Involvement ☐ Tribal Engagement ☐ IMT Coordinator	The SWIC and/or its office has coordinated with 1-4 state/territory agencies responsible for the following emergency communications governance, policy, technology, training & exercise, or usage role at the state/territory level (check all that apply) ☒ 911 – Telephone, CAD, and NG911 ☒ Governance ☒ Training and Exercises ☒ Cybersecurity ☐ Radio Communications Systems ☒ Broadband and Data Systems ☒ Alerts and Warnings ☒ State-level Emergency Management Agency ☒ Priority Telecommunications Services ☒ UASI Involvement ☒ Tribal Engagement ☒ IMT Coordinator

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
6	**Statewide Communication Interoperability Plan (SCIP) Refresh:** SCIP is a planning document that continues to be executed in a timely manner. Updated SCIPs are reviewed and approved by SIGB/SIEC.	The state/territory does not have a SCIP	The state/territory has a SCIP but it is older than three years	The state/territory has a SCIP that has been updated within the past three years.
7	**Completion of SCIP goals:** The state/territory is on track to accomplish the goals laid out in the SCIP and/or has completed the goals within the desired timeframe	<50% of the SCIP goals are completed or on track for completion	>51%<79% of the SCIP goals are completed or on track for completion	>80% of the SCIP goals are completed or on track for completion
8	**Utilization of the Emergency Communications Governing Body to discuss SCIP Progress:** SCIP progress updates are a regular topic for discussion during for emergency communications governing body meetings.	SCIP progress updates are not included as a meeting agenda topic for the emergency communications governing body meetings	SCIP progress updates are included one to two times a year as a meeting agenda topic for the emergency communications governing body meetings	SCIP progress updates are regularly included as a meeting agenda topic for the emergency communications governing body meetings
9	**Integrated Emergency Communication Grant Coordination:** For Federal grants funds, the state / territory is tracking and optimizing emergency communications grant proposals with the assistance of the SWIC to ensure compliance and interoperability with national and state/territory standards, alignment with the SCIP, and there is strategic visibility into how grant money is being spent.	No explicit approach or only informal emergency communications grant coordination between localities, agencies, SAA and/or the SWIC within a state / territory	SWIC and/or the emergency communications governing body provides guidance to agencies and localities for emergency communications grant funding but does not review proposals or make recommendations	SWIC and/or the emergency communications governing body provides guidance to agencies and localities for emergency communications grant funding and reviews grant proposals for alignment with the SCIP and complies with appropriate standards such as P25. SWIC and/or the emergency communications governing body provides recommendations to the SAA.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
10	**TICP (or equivalent) Developed:** Tactical Interoperable Communications Plans (TICPs) are established at the statewide or regional level and are periodically reviewed, validated, and updated (if needed). TICPs are socialized with the appropriate public safety stakeholders and are used during exercises *TICPs are designed to define the breadth and scope of interoperable assets available in the designated area; how those assets are shared; how their use is prioritized; and the steps agencies should follow to request, activate, use, and deactivate each asset.*	No statewide or regional TICP in place	Statewide or Regional TICP(s) have been reviewed, validated, and updated (if needed) within the past 2-5 years but has not been socialized with the appropriate public safety stakeholders or used during exercises	Statewide or Regional TICP(s) have been reviewed, validated, and updated (if needed) within the past 2 years and has been socialized with the appropriate public safety stakeholders and are used during exercises
11	**Field Operations Guides (FOGs) developed.** FOGs established for a state or territory and periodically updated to include all public safety communications systems available	No statewide or regional FOG in place	Statewide or regional FOG(s) have been reviewed, validated, and updated (if needed) within the past 2-5 years but has not been socialized with the appropriate public safety stakeholders or used during exercises	Statewide or regional FOG(s) have been reviewed, validated, and updated (if needed) within the past 2 years and has been socialized with the appropriate public safety stakeholders and are used during exercises

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
12	**Statewide AWN plan:** State/Territory has a statewide Alerts, Warnings, and Notifications plan that highlights the roles and responsibilities of each relevant entities.	No statewide or territory-wide AWN plan	Statewide or territory-wide coordinated AWN plan is in place and is older than 2 years	Statewide or territory-wide coordinated AWN plan is in place and has been reviewed within the last 2 years and describes how all Alerts, warnings and notifications are handled across all alerting authorities.
13	**Outreach to Entities not covered in AWN plan:** State/Territory understand and know who is not covered by the statewide/territory-wide AWN plan and has an outreach plan in place to build partnerships with these entities. *Some examples of entities not covered within an AWN plan are military bases and tribes*	State/Territory knows which entities are not covered in the statewide/territory-wide AWN plan but has not conducted outreach to such entities	State/Territory knows which entities are not covered in the statewide/territory-wide coordinated AWN plan and has conducted outreach to such entities	State/Territory knows which entities are not covered in the statewide/territory-wide coordinates AWN plan, conducted outreach to such entities, and have incorporated these entities into the overall statewide / territory-wide coordinated plan (e.g., MOU)
14	**Radio Programming:** State-owned/state-controlled radios are programmed for National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state / territory.	<49% of state-owned/state-controlled radios are programed for interoperability and consistency	>50%<74% of state-owned/state-controlled radios are programed for interoperability and consistency	>75%<100% of state-owned/state-controlled radios are programmed for interoperability and consistency
15	**Sustainment of Radio Programming:** State/Territory has a radio programming plan	State/Territory has a radio programming plan or are in the process of developing a radio programming plan	State/Territory has a radio programming plan in place and provide trainings to the radio users to help with compliance	State/Territory has a radio programming plan, provides training to the radio users, and has a sustainability mechanism in place *Sustainability mechanism means plans to*

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	developed to ensure radios are programmed for National/Federal, SLTT interoperability channels and channel nomenclature are consist across a state/territory			*maintain and correct radio programming over a long period of time. An example is having a regularly scheduled check of radios to ensure they are programmed as intent.*
16	**Continuous Education of Radio Programming:** State/Territory has a plan in place to continuously educate radio users on National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state/territory	There is no plan in place for continuous education for radio users on radio programming and channel nomenclature	State/Territory is developing a continuous education plan for radio users on radio programming and channel nomenclature	State/Territory has a continuous education plan in place for radio users on radio programming and channel nomenclature
17	**Radio Encryption Plan:** The state/territory has an encryption plan that promotes Advanced Encryption Standard (AES) in place for the radio systems within the state/territory	There is no encryption plan that promotes AES in place for the radio systems within the state/territory	The state/territory is developing an encryption plan that promotes AES for radio systems within the state/territory	The state/territory has an encryption plan that promotes AES in place for radio systems within the state/territory
18	**Cybersecurity Assessment Awareness**: Public safety communications network owners have conducted a cybersecurity assessment and developed a cyber incident response plan. *For this Marker, public safety communications networks are LMR, 911,*	Public safety communications network owners, specifically LMR, 911, and A&W, have started a cyber security assessment. (check the box by for the public safety communication networks that have started a cybersecurity assessment) ☐ LMR ☐ 911 ☐ A&W	Public safety communications network owners, specifically LMR, 911, and A&W, have completed a cyber security assessment. (check the box by for the public safety communication networks that completed a cybersecurity assessment) ☐ LMR ☐ 911 ☐ A&W	Public safety communications network owners, specifically LMR, 911, and A&W, have a cyber incident response plan. (check the box by for the public safety communication networks that have a cyber incident response plan) ☐ LMR ☐ 911 ☐ A&W

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	and A&W			
19	**NG911 Implementation:** NG911 implementation is underway to serve state / territory population.	The state/territory NG911 implementation is in the Legacy or Foundational (Phase I) stages where the ESInet is ready to receive 911 calls from the Originating Service Providers (OSP) via a Legacy Network Gateway	The state/territory NG911 implementation is in the Transitional or Intermediate stages (Phase II) where the ESInet is ready to receive 911 calls in SIP format	The state/territory NG911 implementation is in the End State (Phase III) where the ESInet is ready to receive 911 calls in NG911 format
20	**Artificial Intelligence/Machine Learning Incorporation into 911 Call Centers:** The state/territory is incorporating Artificial Intelligence/Machine Learning (AI/ML) tools into 911 call centers to assist with analyzing the numerous data streams coming into the center.	The state/territory has not or is not considering incorporating AI/ML tools into 911 call centers within the state/territory	The state/territory is currently considering/researching possible AI/ML tools that could be incorporated into the 911 centers within the state/territory	The state/territory has identified AI/ML tools to utilize in their 911 call centers and has begun implementations
21	**Data Operability / Interoperability:** Ability of agencies within a region to exchange data on demand, and as needed, and as authorized. Examples of systems would be: - CAD to CAD - Chat - GIS - Critical Incident Management Tool (i.e. Web EOC) - Patient Care Records (i.e. Transfer of patient from one jurisdiction to the next)	Agencies are able to share data only by email. Systems are not touching or talking.	Systems are able to touch but with limited capabilities. One way information sharing.	Full system to system integration. Able to fully consume and manipulate data. Two-way information sharing
22	**Communications Exercise Objectives:** States/Territories have exercised and successfully tested their capabilities against all of FEMA's Operational	State/Territory has exercised and tested their capabilities against 1 to 2 of the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet. (Check the ones that have been tested in an exercise)	State/Territory has exercised and tested their capabilities against 1 to 2 of the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet. (Check the ones that have been tested in an exercise)	State/Territory has exercised and tested their capabilities against 1 to 2 of the standardized capability targets for Operational Communications as outlined in the FEMA Operational Communications Core Capability Development Sheet. (Check the ones that have been tested in an exercise)

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	Communications Core Capabilities standard capability targets	☐ Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, state and local first responders ☐ Re-establish sufficient communications infrastructure within the affected area to support ongoing life-sustaining activities, provide basic human needs, and a transition to recovery ☐ Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resilience of key systems	☐ Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, state and local first responders ☐ Re-establish sufficient communications infrastructure within the affected area to support ongoing life-sustaining activities, provide basic human needs, and a transition to recovery ☐ Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resilience of key systems	☒ Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, state and local first responders ☒ Re-establish sufficient communications infrastructure within the affected area to support ongoing life-sustaining activities, provide basic human needs, and a transition to recovery ☒ Re-establish critical information networks, including cybersecurity information sharing networks, to inform situational awareness, enable incident response, and support the resilience of key systems
23	**Information and Communications Technology Position Resource Plan:** States/Territories have an Information and Communications Technology Position Resource Plan in place and a process for reviewing and refreshing the plan, as needed. *An Information and Communications Technology Position Resource Plan is the guiding document for the use and deployment of qualified communications unit personnel. Sometimes that plan will also document the process for credentialling or state recognition.*	State/Territory is conducting a communications unit needs assessment and/or developing an Information and Communications Technology Position Resource Plan	State/Territory has an Information and Communications Technology Position Resource Plan	State/Territory has an Information and Communications Technology Position Resource Plan and a process for reviewing and refreshing their Information and Communications Technology Position Resource Plan, when needed
24	**Incident Communications Resource Coordination Process:** Process to develop, maintain, and	☐ State/Territory does not have an active program/process to develop, maintain, and deploy emergency communications resources to support incident communications.	State/territory has an incident communications resource plan, facilitates resource supports an established process for qualification and has an actively engaged resource qualification review board (QRB)	State/territory has an incident communications resource plan, actively engaged QRB, and the state/territory has the ability to deploy/facilitate deployment of incident communications resources

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	deploy emergency communications capabilities is implemented and active in state/territory.	OR ☐ State/Territory offers courses in the relevant Information and Communications Technology (ICT) positions and has active enrollment in these courses.		
25	**Communications Usage Best Practices/Lessons Learned:** Thorough after action reporting, capability and mechanism exists within the state/territory to capture emergency communications best practices/lessons learned activities and share these activities with the appropriate stakeholders and partners.	Does not capture emergency communications best practices/lessons learned activities through after action reporting	Does capture emergency communications best practices/lessons learned activities through after action reporting	Does capture emergency communications best practices/lessons learned activities through after action reporting and proactively shares these activities with stakeholders and partners. *ICAR Question: Do you use the Incident Communications Activity Report (ICAR) or something similar to share emergency communications best practices and lessons learned?* ☐ Yes ☐ No
26	**Promoting Priority Telecommunications Services Best Practices:** SWIC and/or the emergency communications governing body are actively promoting the use of Priority Telecommunications Services (PTS) within the state/territory.	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 1-2 activities (check all that apply): ☐ Promoting PTS by distributing relevant information to stakeholders ☐ Incorporating GETS and WPS into trainings and exercises ☐ Requesting annual training and education on PTS ☐ Including PTS programs and products updates on the emergency communications governing body's meeting agenda	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 1-2 activities (check all that apply): ☐ Promoting PTS by distributing relevant information to stakeholders ☐ Incorporating GETS and WPS into trainings and exercises ☐ Requesting annual training and education on PTS ☐ Including PTS programs and products updates on the emergency communications governing body's meeting agenda	SWIC and/or the emergency communications governing body are promoting Priority Telecommunications Services by the following 1-2 activities (check all that apply): ☒ Promoting PTS by distributing relevant information to stakeholders ☒ Incorporating GETS and WPS into trainings and exercises ☒ Requesting annual training and education on PTS ☒ Including PTS programs and products updates on the emergency communications governing body's meeting agenda
27	**Outreach:** The SWIC and/or the SWIC's office has outreach mechanisms in place to share information across state.	The SWIC and/or the SWIC office's electronic communication (e.g. SWIC email, newsletter, social media, etc.) is distributed to relevant stakeholders on regular basis	Initial plus the SWIC and/or the SWIC office attends in-person/webinar conference/meeting attendance and is an active participant.	Defined plus the SWIC and/or the SWIC office maintains a current and up-to-date web presence that contains information about emergency communications interoperability, the state PACE plan (if one is in place), SCIP, trainings, interoperable radio programming, etc.
28	**Sustainment Management/Planning Cycle:** As the	A sustainment assessment plan is in place and includes establishing an end of life date for state/territory owned or leased interoperable	Meets criteria for Initial, plus established a tool that allows the state/territory to track the sustainment plan for the components of the	Meets the criteria for Defined, plus the state/territory has the administration and support needed to maintain a sustainment

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	technologies' life cycles are getting shorter, states/territories have adapted interoperable component system's sustainment through updated policies and other activities. For example, having an accurate inventory of equipment subject to lifecycle management. *For this Marker, component systems are emergency communications elements that are necessary to enable communications, whether owned or leased - state systems only*	component systems (e.g. communications infrastructure, equipment, programs, management) that need sustainment funding.	state/territory owned or leased interoperable system.	management system for the components of their owned or leased interoperable systems.
29	**Risk Management and Mitigation *(PACE Focus)*:** The state/territory has a Primary, Alternative, Contingency, Emergency (PACE) plan in place that has been socialized and exercised.	The state/territory does not have a PACE plan in place	The state/territory is developing a PACE plan	The state/territory has completed a PACE plan within the last two years and it has been socialized and exercised.
30	**Risk Management and Mitigation (Cybersecurity Focus):** The state/territory has a cybersecurity plan that includes emergency communications technologies in place	The state/territory does not have a cybersecurity plan that includes emergency communications technologies in place	The state/territory is developing a cybersecurity plan that includes emergency communications technologies	The state/territory has completed a cybersecurity plan that includes emergency communications technologies within the last two years and it has been socialized and exercised.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	that has been socialized and exercised.			

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

APPENDIX C: GRANT GUIDANCE 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

Figure 3: SAFECOM Grant Management Suggested Actions/Best Practices

Investment Priorities

National Emergency Communications Plan (NECP) Priorities

The SIEC fully supports the national priorities identified in the most recent version of 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:

- Projects that increase cyber resilience of public safety communications networks and systems implementation of cybersecurity measures identified in a formal system assessment or cybersecurity plan
- Projects that assess the cyber vulnerabilities and/or result in the creation/update of a cybersecurity plan for public safety and emergency communications[7] networks
- Projects that support goals and objectives outlined in the State Homeland Security Strategy.
- Projects that harden, increase the resiliency of, and/or reduce all-hazards risks to public safety communications systems, emergency communications systems[8], and dependent Infrastructure. Examples include but are not limited to:

[7] ORS 403.105 defines "Emergency communications system" as the network, database, servers, other equipment and services that provide the means to communicate with a primary public safety answering point to request and provide assistance to preserve human life or property. For the purposes of this section, public safety communications networks include emergency communications networks, land mobile radio, public safety broadband, and emergency alerts and warning systems. This term is an all-encompassing term meant to describe the entire public safety communications ecosystem.

  - Installation of physical security infrastructure such as fences, cameras, and alarm systems
  - Installation of generators, batteries, solar systems, and fuel storage 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
  - Other projects that mitigate against the risk of natural hazards (Examples include site fuels reduction, installation of ice shields, lightning protection installation, etc.)
- Replacement of non-standard conforming mobile or portable radios with dual or tri-band equipment that meets or exceeds the technical requirements of the most recent version of the ***SAFECOM Grant Guidance*** for use by frontline responders and dispatch centers
- Equipment and training needed to establish SHARES stations for medical facilities that provide emergency, obstetric, surgical, burn, and/or disaster-related services
- Equipment and training needed to establish SHARES stations for county and tribal emergency operations centers and public safety answering points
- Caches of dual/tri-band radios [9] for use during a disaster, terrorist attack, or large-scale emergency
- Deployable communications equipment including tactical repeaters, gateways, antennas, power systems, satellite connectivity (low earth orbit), and devices designed to make use of the 3GPP MCPTT standard, and associated accessories
- Dedicated staff to increase interoperability and regional interagency cooperation within the emergency communications ecosystem, and communications between PSAPs/Public Safety Dispatch Centers, EOCs, and other critical facilities. Investments should be targeted towards projects that support underserved rural areas and/or where tribal involvement may be better facilitated
- Funding subsequent phases of multi-phased projects previously funded and successfully carried out that continue to align with the SCIP
- Funding for Next-Generation 911 planning, implementation, and deployment.
- Continued funding of OR-Alert
- Continued funding of the SIEC and the Statewide Interoperability Program
- Funding of the Oregon Emergency Response System (OERS) Communications Center
- Refurbishment, update, and maintenance of the State's Strategic Technology Reserve, as well as funding for training and exercise related to the 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 support multi-agency, regional, and/or statewide strategic planning efforts related to emergency and public safety communications

[9] Radio equipment must meet or exceed the technical requirements in the most current version of the ***SAFECOM Grant Guidance***

- Projects that enhance public safety's ability to detect, respond to, and mitigate sources of intentional and unintentional interference (jamming)

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. The lowest priority should be given to projects that only impact a singular agency. Priority should also be given to projects that leverage or expand existing infrastructure, either through the state or regionally, whenever possible.
- Priority should be given to projects that address identified gaps in capabilities through a formal assessment or promulgated plan.
- Priority should be given to projects that support goals and objectives identified within the Statewide Communications Interoperability Plan.
- Projects accompanied by letters attesting to pre-coordination with the Office of the Statewide Interoperability Coordinator and the SIEC's Technical Committee.

Funding Requirement Recommendations

It is SIEC's recommendation that grant funding administered by any state or federal agency operating within Oregon related to any emergency communication project should include the following requirements:

- Coordination with the Office of the Statewide Interoperability Coordinator and the SIEC's Technical Committee early in the project development process. Coordination with other entities may be necessary, depending on the nature of the project.
- Identification of the project in a jurisdiction or region's Strategic Communications Plan, Hazard Mitigation Plan, Community Wildfire Protection Plan, Dam Safety Plan, or other strategic all-hazards preparedness plans, a recent real-world incident after-action report, an exercise improvement plan, and/or within a state-level plan such as the Statewide Communications Interoperability Plan, the State Homeland Security Strategy, the State of the State Capabilities Report the Comprehensive Emergency Management Plan, or similar. If unsure whether a project has been identified in such a plan, please consult with the Office of the Statewide Interoperability Coordinator for guidance.
- Demonstrate that a lifecycle funding plan has been identified for any equipment/infrastructure investments.
- A full project plan with timelines, budget, and milestones identified be developed as part of the application process, unless the application is for planning support.
- For radio equipment purchased with grant funding, the programming of national interoperability channels and public safety mutual aid channels shall be programmed as listed in the most current version of the National Interoperable Field Operations Guide for all bands the radio can operate on.
- For standards based (P25) radio equipment purchased with grant funding, equipment must be on the Department of Homeland Security's P25 Compliance Assessment Program Authorized Equipment List and meet the encryption standards as tested.

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 of 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, software, or services offered by an entity identified by the State Chief Information Officer that may pose a national security threat in accordance with OAR 128-020-0010.
    - Certain law enforcement purchases for specific purposes may be exempt.
- Equipment or services offered by certain telecommunications providers identified in Section 2 of the Secure Networks Act.
- 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.
- GMRS and FRS equipment under an emergency communications justification. [10]
- Amateur radio equipment that is not utilized for HF SHARES, or not installed in public safety command posts, public safety, answering points, or emergency operations centers where standards-based equipment is also installed. [11]

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

[10] This type of equipment may qualify under community resilience or similar justifications.

[11] The purchase of amateur radio equipment for other purposes may be permissible under investment justifications other than "emergency communications" which are not subject to SCIP and SAFECOM Grant Guidance Compliance/SWIC Review.

- Oregon Homeland Security Grant Program
- Assistance to Firefighters Grant Program
- Tribal Homeland Security Grant
- Port Security Grant

APPENDIX D: PRIORITIES IDENTIFIED IN THE NATIONAL EMERGENCY COMMUNICATIONS PLAN (NECP)

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 Information Communications Technology Branch 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