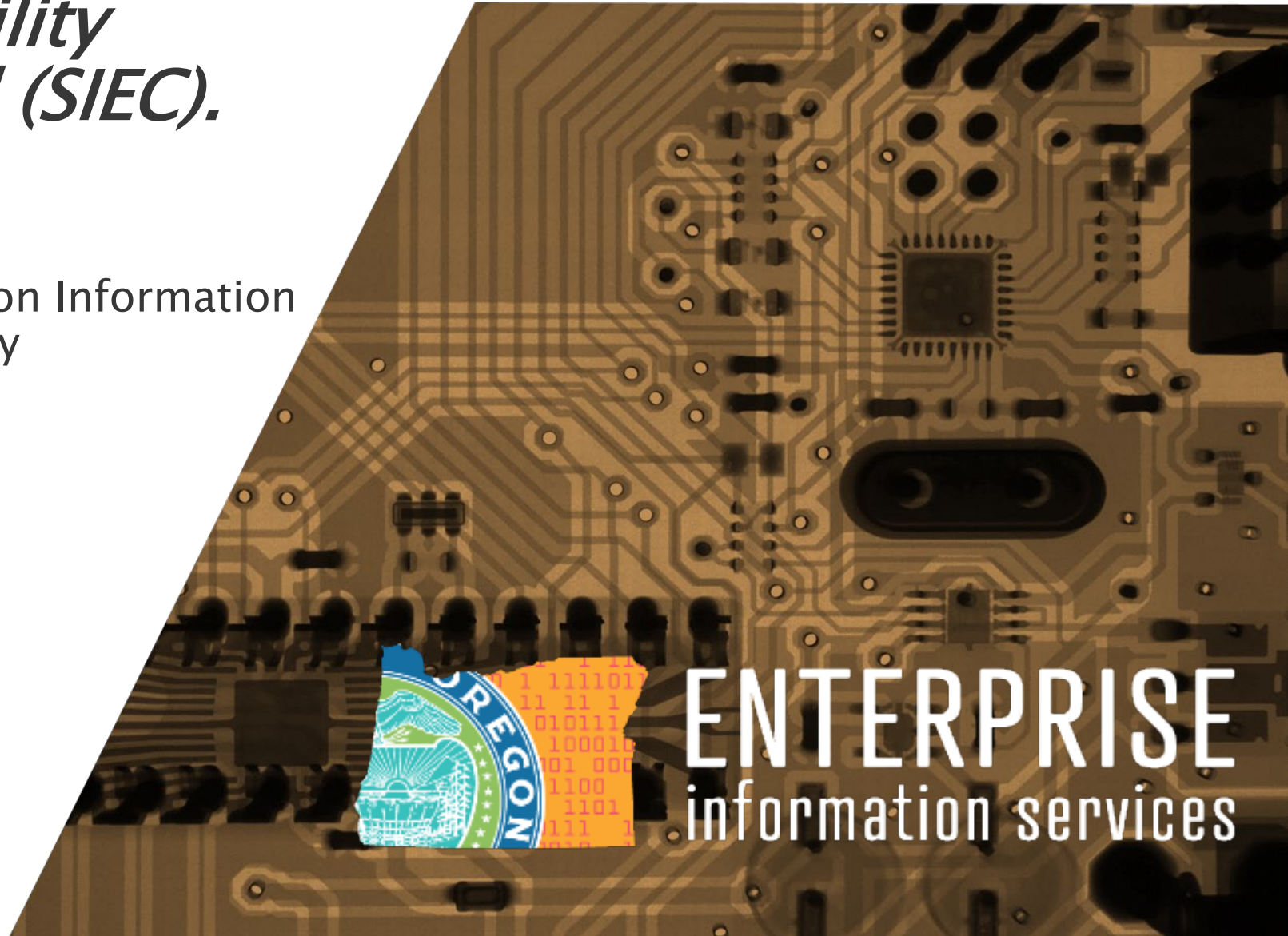


State Interoperability Executive Council (SIEC). Update

Joint Legislative Committee on Information
Management and Technology

*William Chapman
Mike Duyck
Ben Gherezgiher*

10 March 2021



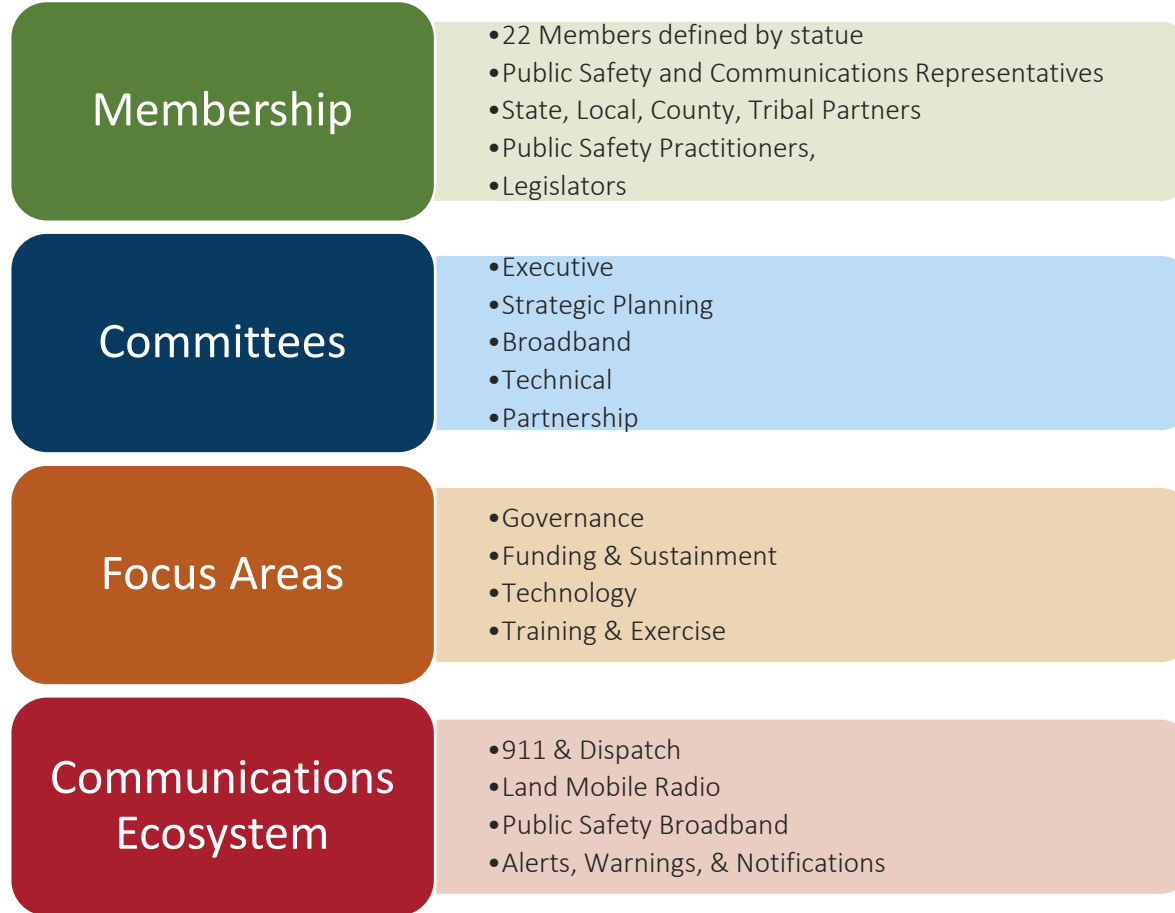
SIEC and the Statewide Interoperability Program



ENTERPRISE
information services

Background. *Statewide Interoperability Executive Council (SIEC)*

“Seamless interoperable emergency communications” - an interdisciplinary, whole community approach to interoperability



SIEC Established in 2002 by Executive Order.
Codified in 2005 under ORS 403.450



ENTERPRISE
information services

SIEC. *Charter, Accomplishments, and Success Indicators*

The Council Charter

- Foundational guidance document for the SIEC
- Defines the overarching principles and structure of the SIEC
- Defines the mission of the SIEC in alignment with ORS 403.450
- Outlines SIEC success indicators

Historic Accomplishments

- ✓ **FirstNet.** Establishment and development of the statewide plan for FirstNet
- ✓ **SCIP.** Implementation of State Communications Interoperability Plan (SCIP)
- ✓ **Collaborative Forum.** Key driver of interoperability efforts within the State

Success Indicators for the SIEC

- **Awareness.** Stakeholders and beneficiaries are aware of SIEC and SCIP
- **Agreement.** There is a consensus on issues of interoperability
- **Alignment.** Oregon meets or exceeds requirements from the National Emergency Communications Plan (NECP)
- **Leadership.** The SIEC becomes a leader, standard-setter, and statewide resource
- **FirstNet Implementation.** Oregon coordinates activities required for the successful implementation of FirstNet throughout Oregon
- **Continuous Improvement.** There is measurable improvement in interoperability and the sustainability of critical communications infrastructure

Operability vs. Interoperability

- **Operability** – Ability to provide and maintain reliable communications functionality throughout the area of responsibility.
- **Interoperability** – Ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized.



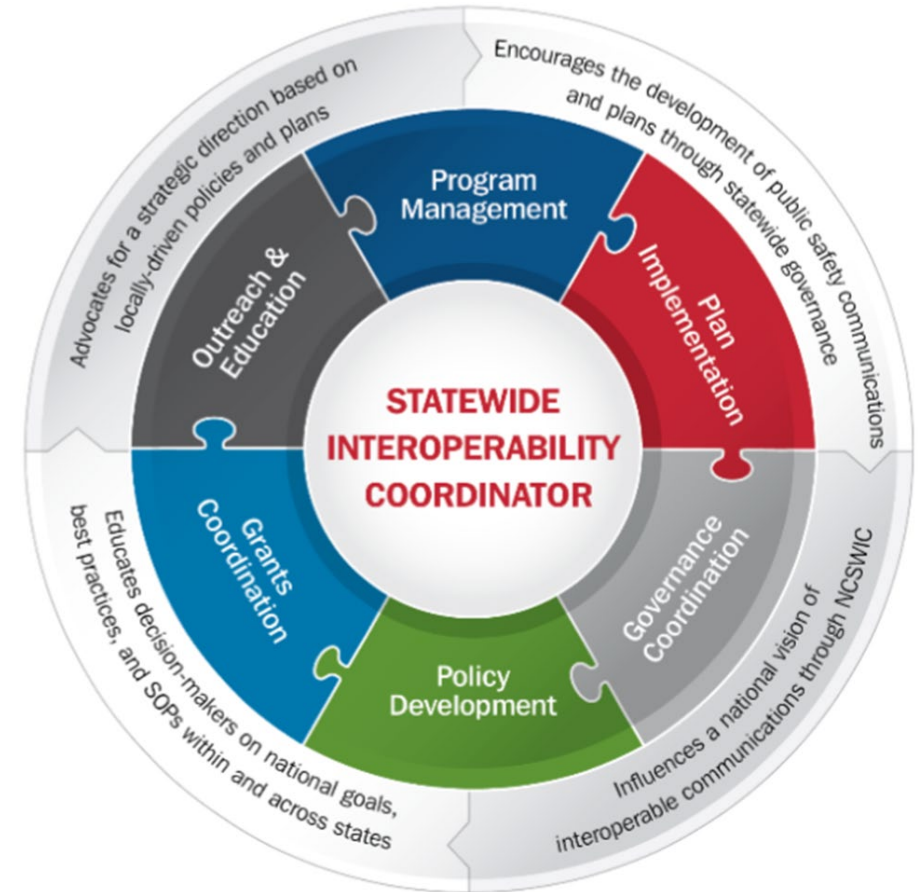
SIEC. *Committee Structure*



Statewide Interoperability. *Program and SIEC*

Statewide Interoperability Coordinator (SWIC)

- **Enabling Legislation.** Established under Enterprise Information Services (EIS) pursuant to ORS 403.460*
- **Role.** Serves as the primary point of coordination for all statewide interoperable emergency communications efforts; and mediates disputes amongst public bodies
- **Duties.** Supports the *State Interoperability Executive Council* (SIEC) and assists with the update and implementation of the *State Communications Interoperability Plan* (SCIP)
- **Representation.** Serves as a member of the *National Council of SWICs* (NCSWIC)**

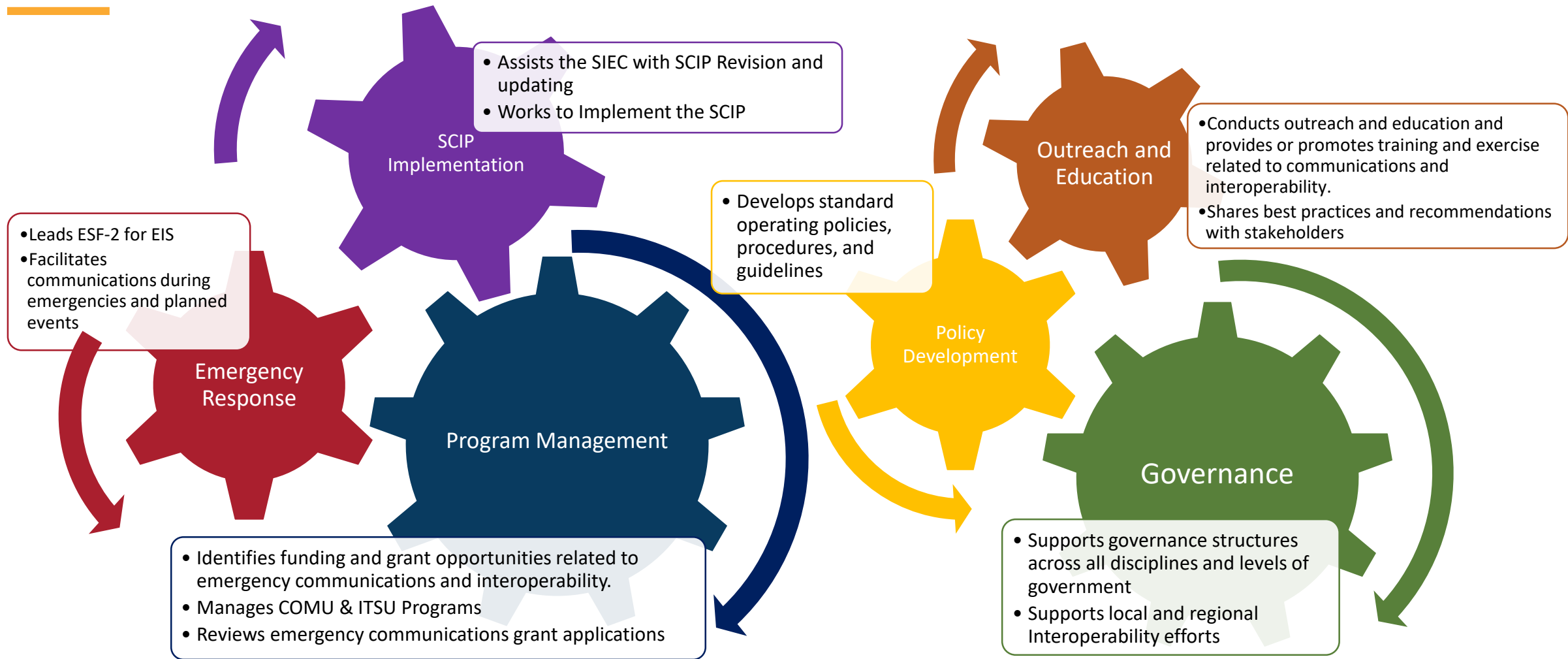


*Previously the SWIC has been housed within the Oregon State Police, Office of Emergency Management and the Oregon Department of Transportation

**Each state/territory has a designated SWIC



Statewide Interoperability. *What does the SWIC do?*



Statewide Interoperability. *Top Priorities*

OR-Alert

- Implementation for all Counties
- Establish Governance Committee
- Develop Statewide Alerts and Warnings Best Practices Guide

COMU

- Begin Certifying Trainees
- Establish In-State Training Cadre
- Build Relationships

NG-911

- Develop Strategic Plan
- Create Sub-Working Groups
- Obtain Funding & Support for Implementation

“Interoperability begins with relationships”



ENTERPRISE
information services

Statewide Interoperability. *Significant Activities*

- ✓ Update of Oregon State Interoperability Markers Assessment
- ✓ **2020 Statewide Communications Interoperability Plan (SCIP) Update**
- ✓ **Establishment of All-Hazards Communications Unit Program**
 - ✓ Communications Unit Leader Training
 - ✓ Auxiliary Communicator Training
 - ✓ Incident Tactical Dispatcher Training
 - ✓ Comms Exercise planned for June
 - ✓ Integrated with Telecommunicators Emergency Response Team (TERT)
- ✓ Emergency Communications Grant Funding Webinar
- ✓ **Statewide Alerts and Warnings System (OR-Alert)**
- ✓ Federal Interoperability Channels MOU
- ✓ Tactical Interoperable Communications Field Operations Guide (TIC-FOG) Update
- ✓ Cybersecurity Training for PSAPs
- ✓ Incorporation of Oregon Statewide Cyber Disruption and Response and Recovery Plan Goal into SCIP
- ✓ **Formation of the Washington/Oregon Regional Joint Interoperability Committee (WORJIC)**
- ✓ Deployment to the State ECC in support of COVID-19 Response, Wildfires, & Winter Storms
 - ✓ Supported Oregon Medical Station and Vaccine Clinics at Fairgrounds
 - ✓ Supported OEM's move to DPSST
 - ✓ ESF-2 Coordination Calls and Sit Reps
 - ✓ Public-Private coordination with cellular & broadband providers, public safety radio systems, 911 centers, and emergency managers.
 - ✓ Supported 15 Seat Call center in support of OED
 - ✓ Supported 6 Seat Call center in Support of Gov's Office
 - ✓ Supported Communications for Wilsonville Distribution Facility
 - ✓ Integrated with Federal ESF-2 for intergovernmental support
 - ✓ Coordination of Communications Critical Infrastructure Protection
 - ✓ Coordinated out-of-state communications support.



Statewide Interoperability. *OR-Alert*



Mass Notification with Incident

Communications. Enabling local and statewide alerts and warnings across 25+ channels using GIS-based message targeting, and providing templates that automate recipients and content based on location, incident type and severity—reducing error and ensuring message integrity*



Community Engagement.

Enabling anonymous opt-ins to state and local notifications using keywords or ZIP codes, and providing one-click publishing across all channels*



SMARTWeather. Specific, map-driven, targeted, rules-based and automated weather alerts from the National Weather Service*



PREPARE

RESPOND

RECOVER

OR-Alert Mission - *Ensure access to timely and informative alerts, warnings and notifications (AWNs) through implementation of a statewide system that enables state, county, city and tribal governments to issue Awns—providing people in Oregon with meaningful opportunities to make life-saving decisions in the face of emergencies*

*For additional information see the [Mass Notification Data Sheet](#), the [Community Engagement Data Sheet](#) for additional details, and the [SMARTWeather Data Sheet](#) for additional details on features and capabilities



ENTERPRISE
information services

Statewide Interoperability. *Cybersecurity Training*

PROTECT YOUR CENTER FROM RANSOMWARE



OREGON STATE INTEROPERABILITY PROGRAM

RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive; there are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

- 1** Contact your IT department and supervisor immediately
- 2** If you can locate the Ethernet cable, unplug the computer from the network
- 3** If you can't disconnect the computer from the network, unplug it from power
For laptops: hold down the power button until the light is completely off and remove the battery if possible

IMPORTANT CONTACTS

STATE OF OREGON

- Oregon Cybersecurity State Incident Response Team
(503) 378-5930 eso_soc@oregon.gov
- Oregon Emergency Response System (OERS) 1-800-452-0311
- State Interoperability Program
(503) 373-7251 william.chapman@oregon.gov

WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.



Note To Users:

Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.



The Federal Government advises organizations **NOT** to pay any ransom. Organizations should maintain off-site, tested backups of critical data.

If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance

FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA)
(888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI Portland Field Office
(503) 224-4181
- FBI Internet Crime Complaint Center (IC3)
www.ic3.gov
- FBI Field Office Cyber Task Forces
www.fbi.gov/contact-us/field

PROTECTING YOUR CENTER

Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.

PHISHING

Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.

- ✓ Be suspicious of any email asking you to follow a link or open an attachment
- ✓ If you are not expecting an email attachment from a co-worker, give them a call to verify
- ✓ Report suspicious emails to your IT staff
- ✓ Never check personal email from computers with access to Computer Aided Dispatch (CAD), Records Management System (RMS), or other mission critical systems
- ✓ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different—this is a red flag
- ✓ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

SOCIAL ENGINEERING

Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trusted relationships.

- ✓ Remove any work-related information from your social media accounts
- ✓ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ✓ Be suspicious of emails from coworkers and friends asking you to click a link or open an attachment

DRIVE-BY-DOWNLOAD

Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious site will enable malware or ransomware infection.

- ✓ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ✓ If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled
- ✓ Web browsing should be limited to websites related to your mission and job responsibilities

USERNAME & PASSWORD COMPROMISE

Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain access to your agency's network. If your password is too simple, it can also be easily guessed.

- ✓ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ✓ Don't reuse passwords across different accounts and online services
- ✓ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, Etc)

Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave thumbdrives in public places hoping you will insert them into your computer.

- ✓ Never connect USB devices to CAD, RMS, or other mission critical systems
- ✓ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet



ENTERPRISE
information services

Statewide Communications Interoperability Plan. *Goals*



Strategic & Ongoing

- Conduct outreach and education across various levels of government
- Promote awareness of public safety personnel about the exercise and use of LMR, public safety broadband, 911, and alerts and warnings guiding documents.

Short Term

- Assess the emergency communications radio systems in Oregon
- Establish a COMU Program

Mid-Term

- Identify critical stakeholders in the realm of LMR and provide recommendations and best practices.
- Advocate for continued funding of the SIEC

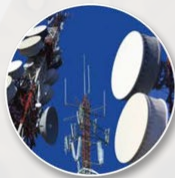
Long Term

- Advocate for statewide efforts to develop and adopt NG-911 in Oregon
- Maintain grant funding requirements



ENTERPRISE
information services

FirstNet Update



ENTERPRISE
information services

FirstNet. *At a Glance*



FirstNet will serve...



IN



ACROSS



Technology first responders need to save lives, protect communities

MODERNIZED

innovative
app & device
ecosystem



network
improvements
& upgrades



commercially proven
cybersecurity
solutions

PRIORITIZED



emergency
communications receive
highest priority

rapid buildout
with public safety
input



nationwide
public safety
solutions
leveraging
existing
infrastructure

SPECIALIZED

robust coverage
where public safety
needs it



connectivity for
advanced
mobile data

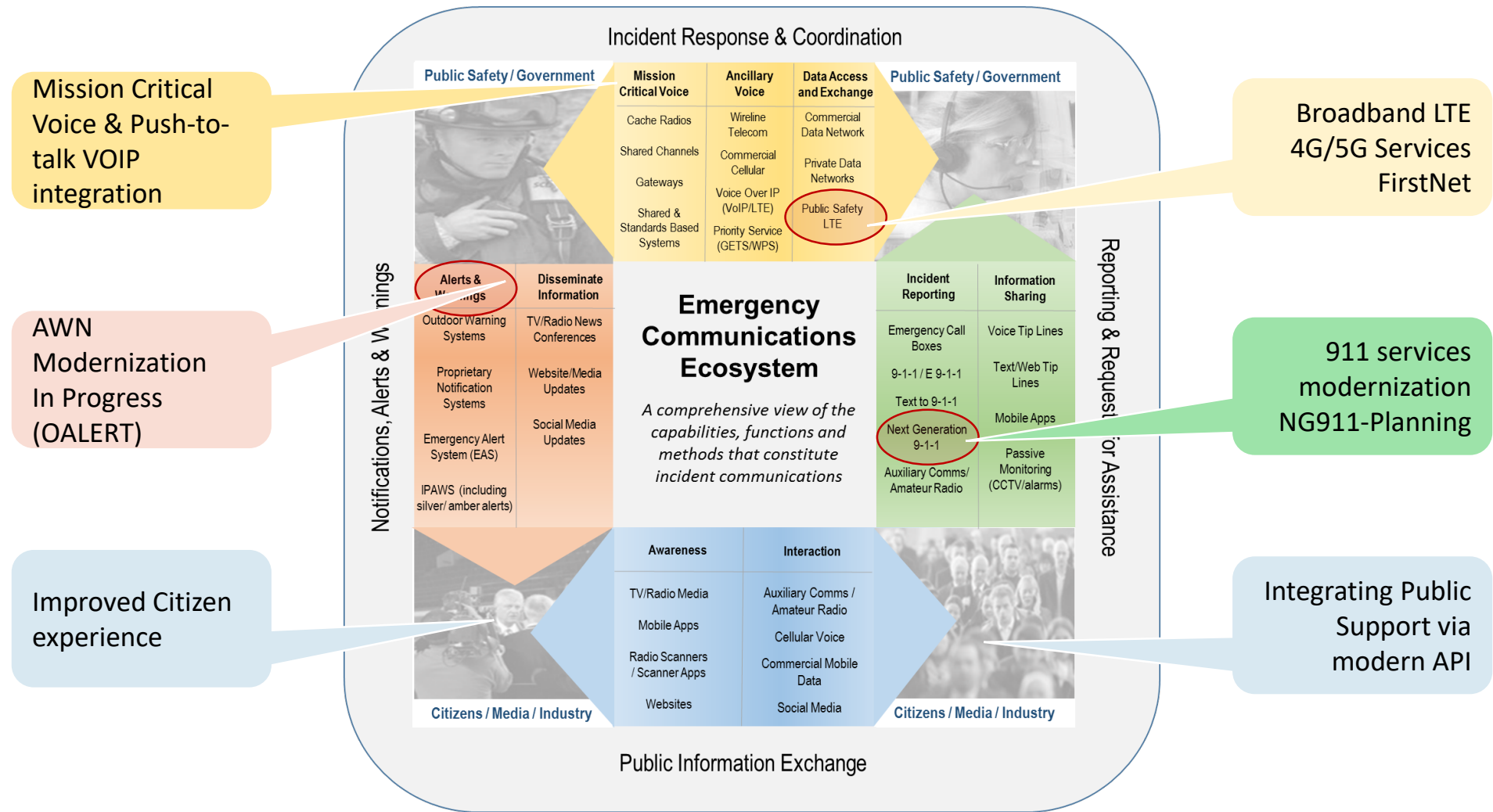


highly available
customer care



ENTERPRISE
information services

Context. *FirstNet and the Communications Ecosystem*



FirstNet. *Facts*



FirstNet is unlike any other network, because it is the only network dedicated to the public safety community. FirstNet is also the only network overseen by the First Responder Network Authority, the independent agency established by Congress to deliver public safety's nationwide broadband network.



First Responder Network Authority® - This logo represents the First Responder Network Authority organization



This logo represents the FirstNet network and services, built with AT&T



FirstNet Roadmap. *Domains and Priorities*



CORE

- Generational Updates (e.g., 4G to 5G)
- Priority and Preemption, including Uplift on 5G
- Mission Critical Services Platforms and Enablers on 5G
- Network Security on 5G



COVERAGE

- Outdoor Coverage Expansion
- Indoor Coverage Expansion
- Unique Coverage Solutions Advancement



SITUATIONAL AWARENESS

- Locate and Present Personnel Location
- Location Services Integration



VOICE COMMUNICATIONS

- Operationalize FirstNet Push-to-Talk
- Active Role in Standards
- Critical Features



SECURE INFORMATION EXCHANGE

- Database Integration
- Application Integration



USER EXPERIENCE

- Mission-Enabling Applications
- Mission-Capable Devices

[FirstNet Authority Roadmap 2020](#)



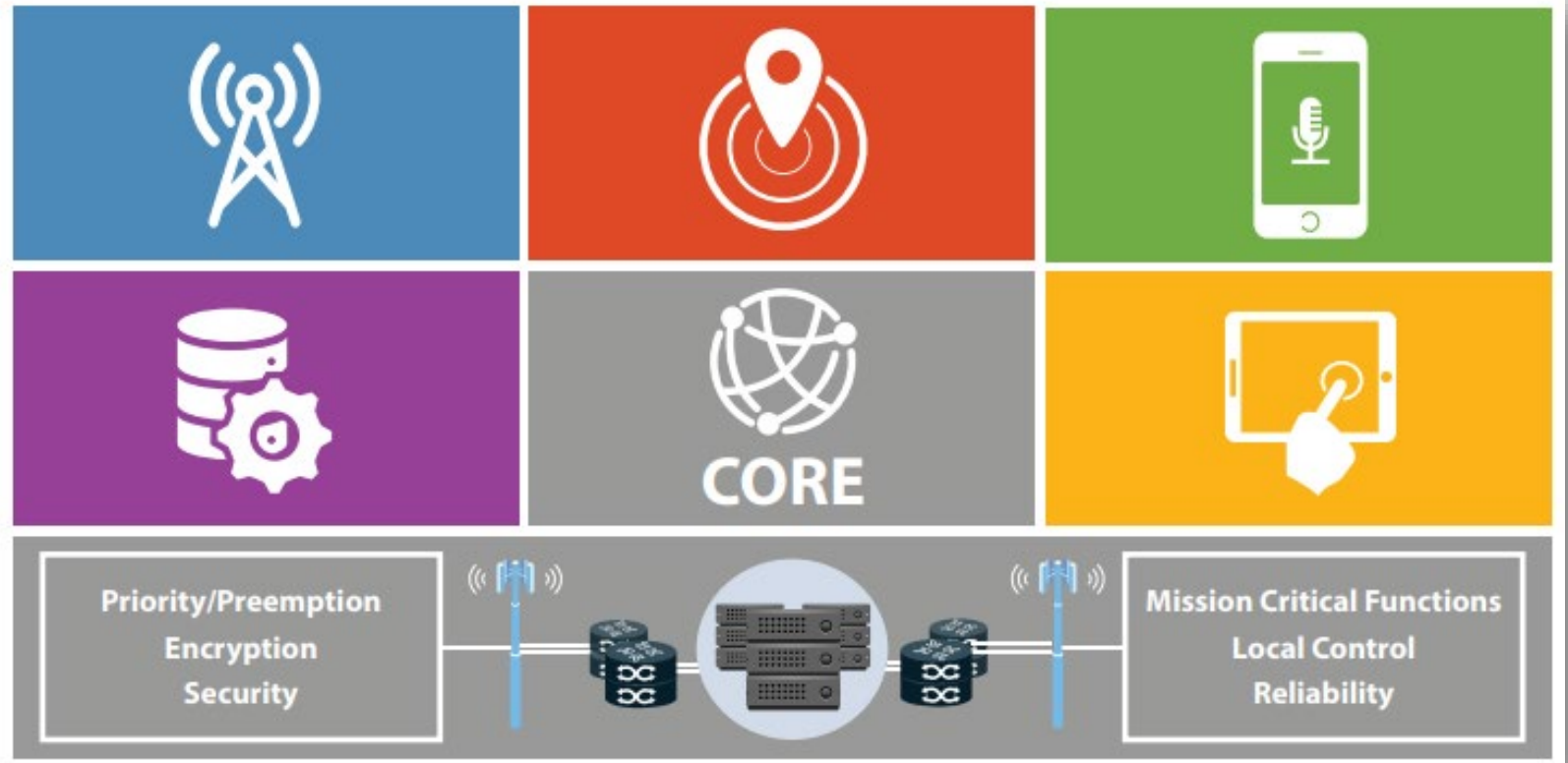
ENTERPRISE
information services

FirstNet Roadmap. *Core*



CORE

- Generational Updates (e.g., 4G to 5G)
- Priority and Preemption, including Uplift on 5G
- Mission Critical Services Platforms and Enablers on 5G
- Network Security on 5G



ENTERPRISE
information services

FirstNet Roadmap. *Coverage*



Deployables



Outdoor Coverage



Drone/Airborne Coverage



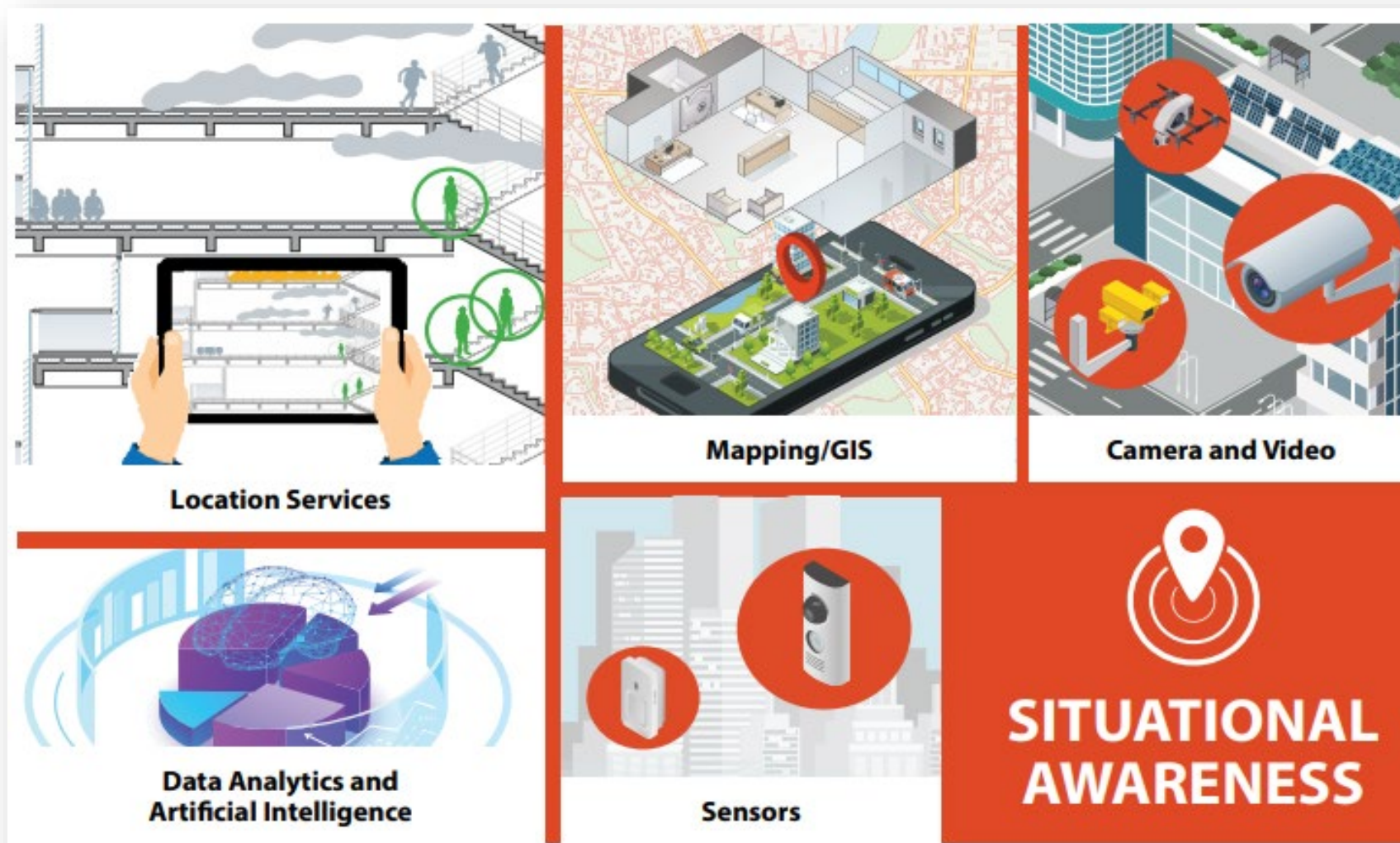
In-building Coverage



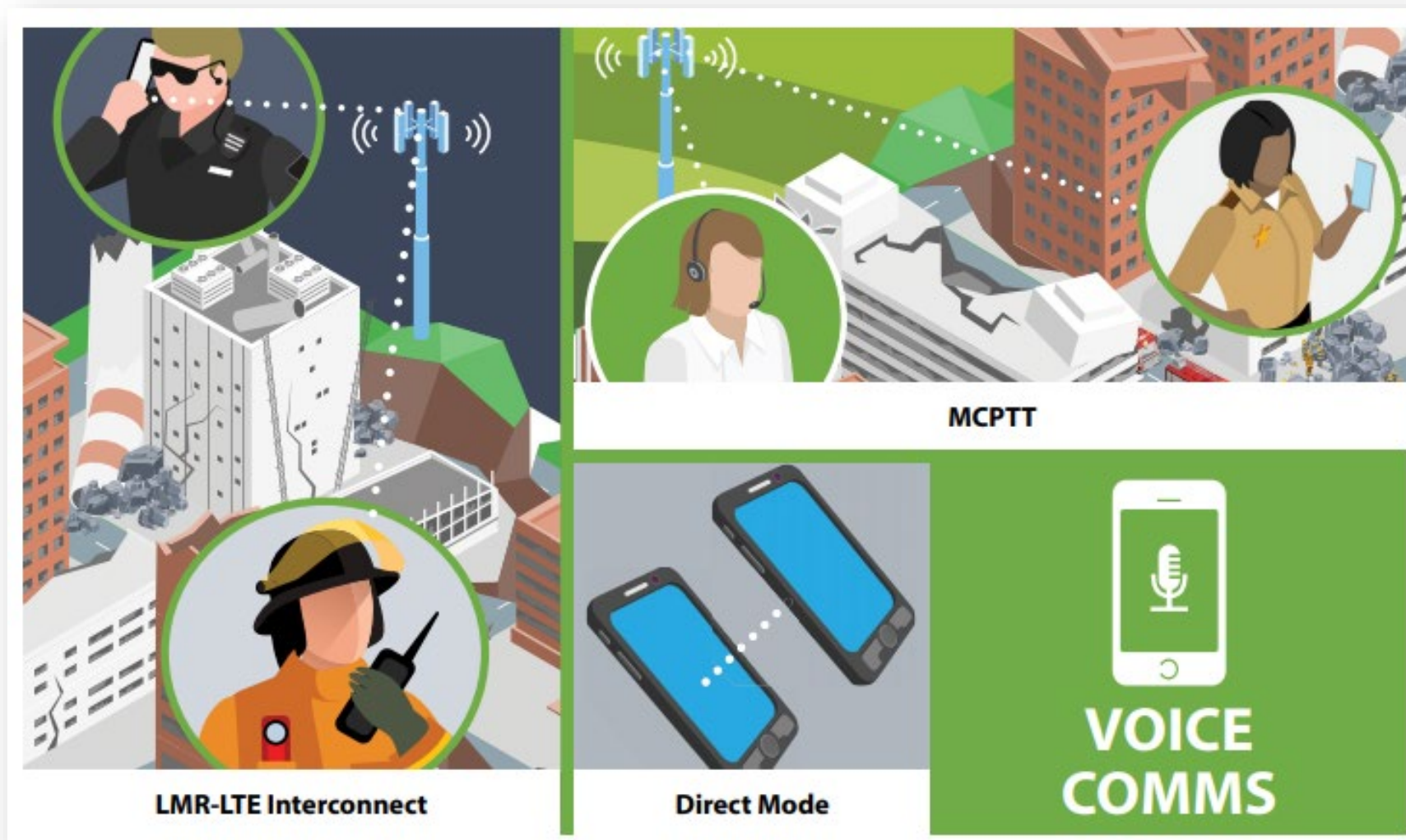
Maritime Coverage



FirstNet Roadmap. *Situational Awareness*



FirstNet Roadmap. *Voice Communications*



FirstNet Roadmap. *User Experience*



FirstNet Roadmap. *Secure Information Exchange*



**Secure Data Sharing, Data Access,
and Identity Management**



Cybersecurity



**SECURE
INFORMATION
EXCHANGE**



ENTERPRISE
information services

FirstNet. *National Dashboard*



FIRSTNET. Built with AT&T **BY THE NUMBERS**

The **only** dedicated communications platform in the country that brings public safety:



Always-on, 24x7 priority and preemption across voice and data communications



A physically separate network core **fully dedicated** to public safety



Government oversight and accountability from the **FirstNet Authority**

Updated: 1/28/2021

¹ Markets defined by FCC CMAs.

©2021 AT&T Intellectual Property. All rights reserved. FirstNet and the FirstNet logo are registered trademarks and service marks of the First Responder Network Authority. All other marks are the property of their respective owners.

1.9M+

FirstNet connections



15K+

Public safety agencies and organizations subscribed



150+

apps in the FirstNet App Catalog



180+

FirstNet Ready™ devices

For Public Safety, By Public Safety

2.61M+

Square miles of LTE coverage nationwide



120K+

Square miles of LTE coverage added in 2019



76+

 Dedicated deployable network assets, including Flying COWs™ and FirstNet One.

80%+

Band 14 coverage completion; well ahead of schedule



700+

Markets¹ with Band 14 spectrum

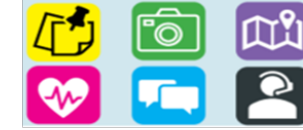


ENTERPRISE
information services

Firstnet. *Oregon Dashboard*



Adoption: 16,500 entities subscribing



RAN Buildout Activities – State Plan

17 sites on air out 45 site target



38% Complete

RAN Buildout Projection – 2021

Total of 28 sites projected to be completed.



- **10 sites under construction**



- **18 sites build projected**

2018 – 2020 Site Resiliency Enhancements RAN Buildout

43 sites had backup generators installed

812 speed & capacity enhancements

249 of them were band 14 add-ons



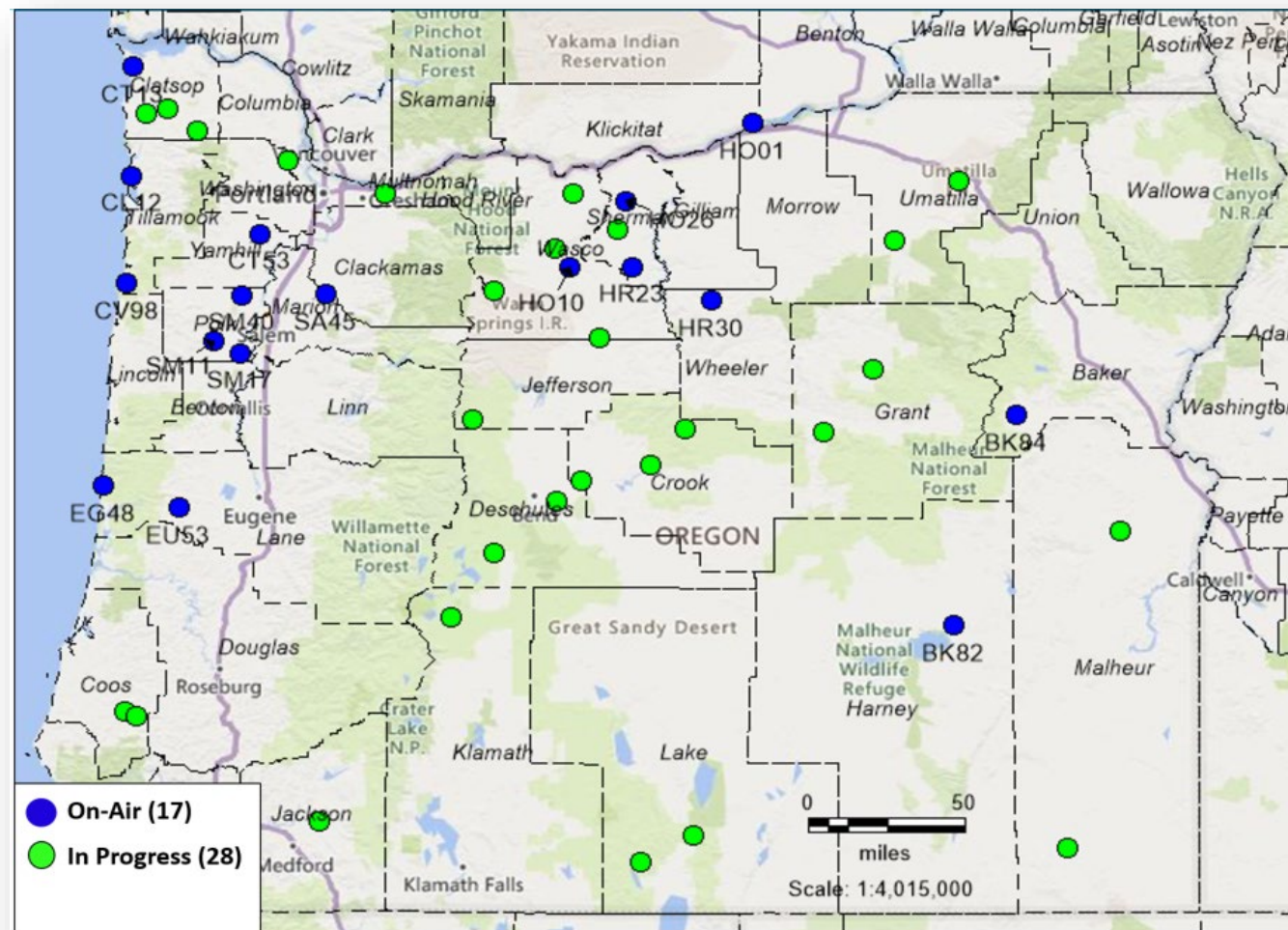
ENTERPRISE
information services

FirstNet in Oregon. *As of December 2020*



Ran Buildout Update

- 17 sites on-air
- 18 sites by Q4 of 2021
- 10 sites in construction

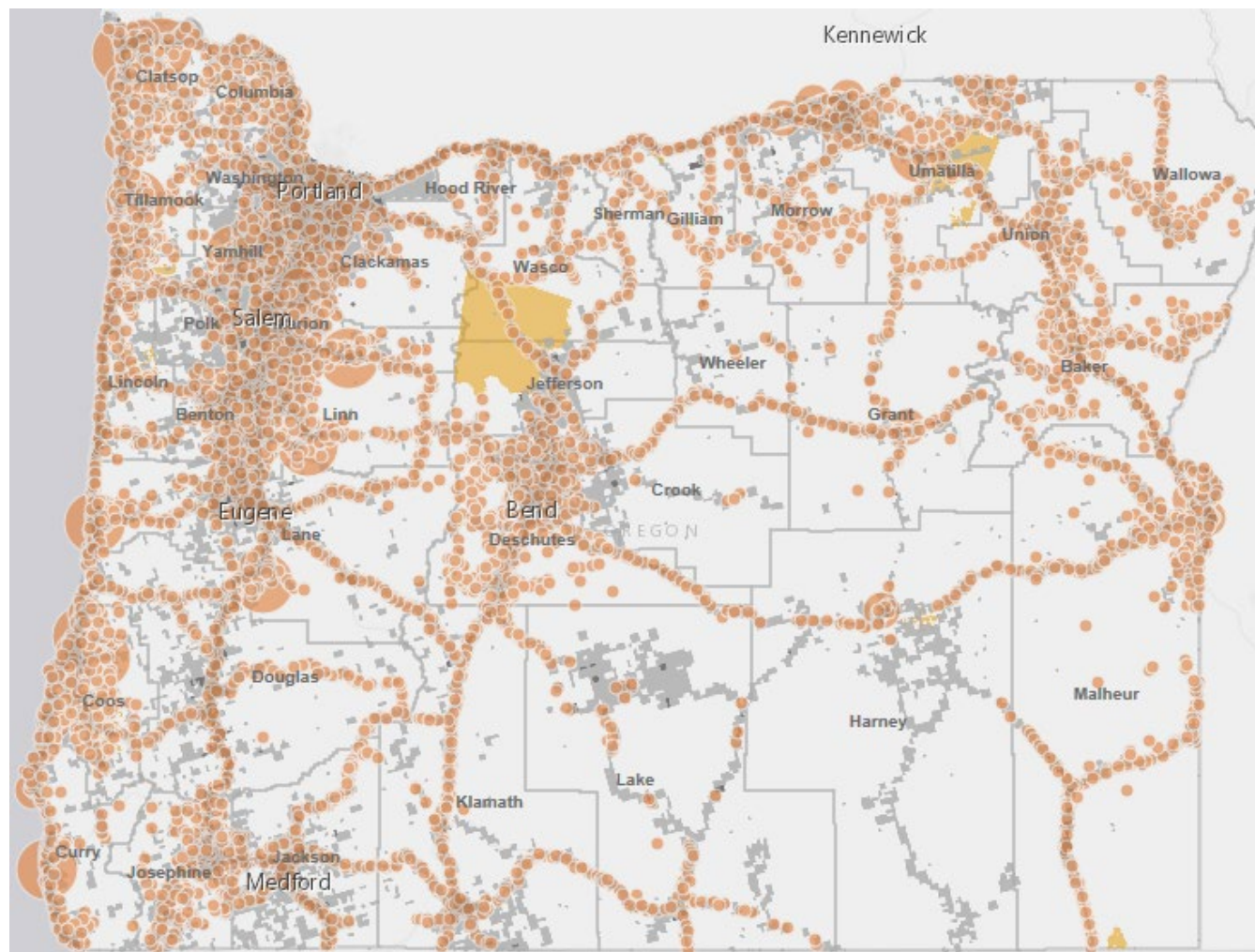


FirstNet in Oregon. *As of December 2020*



Oregon Public Safety Activity Data

- Dispatch 911 calls
- Law enforcement CAD data
- Fire assistance calls
- Medical emergency data

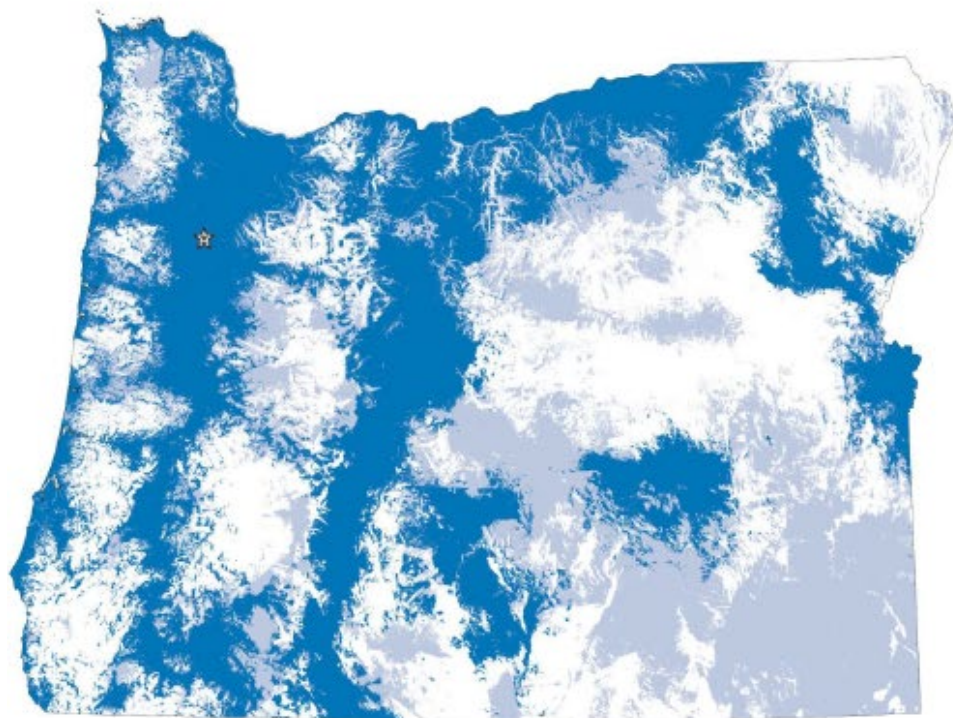


ENTERPRISE
information services

FirstNet in Oregon. *As of December 2020*



Coverage on 5/30/2018

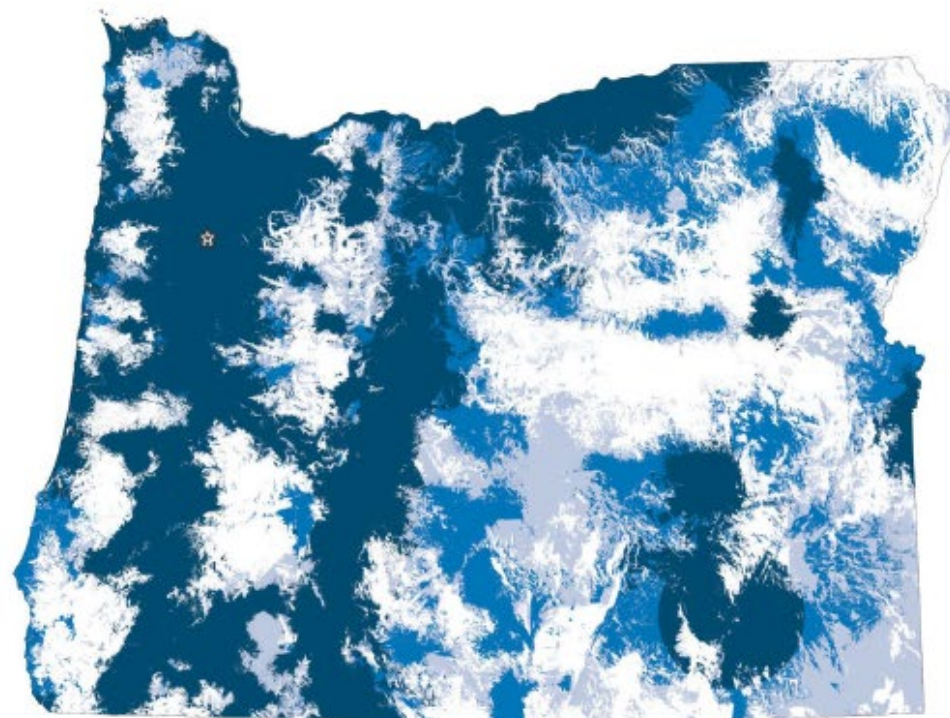


N
Miles 0 40 80
Coverage is displayed at the contractually required signal levels. Band 14 at -122dB and Non-Band 14 (LTE and Other Non-Band 14) at -110dB.



Non-Band 14
LTE with Priority/Preemption
(on 5/30/2018)
Other Non-Band 14
(on 5/30/2018)

Coverage as of 12/31/2020



N
Miles 0 40 80
Coverage is displayed at the contractually required signal levels. Band 14 at -122dB and Non-Band 14 (LTE and Other Non-Band 14) at -110dB.

Band 14
B14 On-Air
(as of 12/31/2020)
Salem

Non-Band 14
LTE with Priority/Preemption
(as of 12/31/2020)
Other Non-Band 14
(as of 12/31/2020)

Use or disclosure of the data on this page or screen is subject to the restrictions on the title page of this document or file.



ENTERPRISE
information services

FirstNet in Oregon. *Fire Emergency Deployment*



❑ 11 Deployments of Satellite Cells On Light Trucks (SatColts) + Generators in 3Q2020

1. First Responder Relief Center, Salem, OR – FirstNet: Launch date: 9/30/2020
2. Holiday Farm Fire, Blue River, OR – FirstNet: Launch date: 9/28/2020
3. Holiday Farm Fire, McKenzie Bridge, OR– FirstNet: Launch Date: 09/28/2020
4. Holiday Farm Fire, Vida, OR– FirstNet : Launch Date: 09/28/2020
5. Hunter Fire, Blanchard, OR– FirstNet : Launch Date: 09/15/2020
6. Holiday Farm Fire, Springfield, OR– FirstNet : Launch Date: 09/15/2020
7. Lionshead Fire, Detroit, OR– FirstNet : Launch Date: 09/12/2020
8. Beachie Creek Fire, Gates, OR– FirstNet : Launch Date: 09/09/2020
9. Holiday Farm Fire, Blue River, OR– FirstNet : Launch Date: 09/08/2020
10. Lionshead Fire, Warm Springs, OR– FirstNet : Launch Date: 08/26/2020
11. Green Ridge Fire, Camp Sherman, OR– FirstNet : Launch Date: 08/19/2020



FirstNet. *State Agency COVID Emergency Support*



- 18 State Agencies received active FirstNet services related to COVID Emergency Support
- We have FirstNet enabled emergency support assets that are managed by the State SWIC that have been in use for multiple emergencies in Oregon.

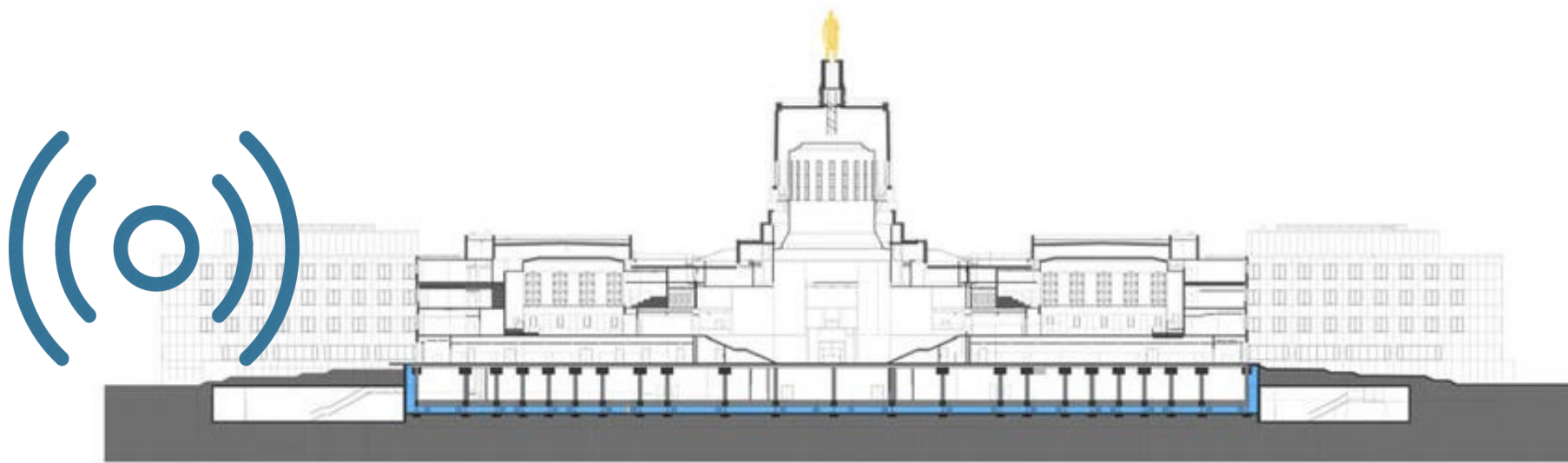


State Buildings. *RF Enhancements*

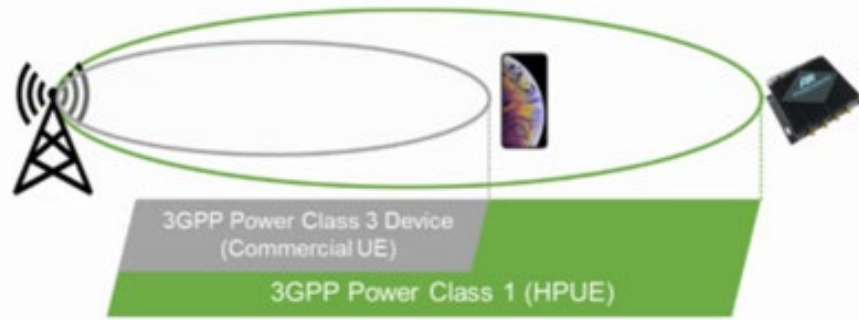


State facilities receiving in-building RF enhancements

- Department of Public Safety Standards and Training – *ready*
- Department of Justice (Portland Building) – *ready*
- Oregon State Police – *planning in progress*
- State Capitol – *planning in progress*



FirstNet . *Technology Enhancements*



FirstNet ready HPUE* antenna rolled out for public safety use, built and FCC licensed specifically for Band 14 ONLY



Mission Critical Push to Talk (PTT)



FirstNet – Z-Axis location services for Public Safety

* HPUE stands for High Powered User Equipment



FirstNet. *Next Steps & Challenges*



FirstNet is still growing as an organization and the national public safety network is progressively being implemented in all 50 states and territories. However, we have experienced some challenges with the network that FirstNet is trying to remedy, including:

- Resiliency Challenges, we have experienced service outages in critical emergency situations.
- While communication from our FirstNet teams was admirable during the outages, still a public safety grade resilient service is expected by first responders in Oregon.
- We had full visibility online and offline and the FirstNet teams recovered all major sites with effective speed.
- Before the project closure we would like to see more backup and recovery implementation on all major sites in Oregon.



FirstNet in Oregon. *Team of Teams*



FirstNet Authority Team

Meet the Public Safety Advocacy Team for the North Region



Lesia Dickson



Tim Pierce



John Hunt



Kyle Richardson





Kristi Wilde




Jon Lewin


AT&T FirstNet Team



George Granger
President – AT&T Oregon



Jake Westlund
FirstNet Outreach Manager – Pacific States




Paul Braunstein
FirstNet Consultant – State of Oregon



Kiley Breitling
FirstNet Consultant – Southern Oregon



Kyle Abernethy
FirstNet Consultant – Eastern Oregon



Amber Blackmon
Regional FirstNet Consultant – Pacific States

SIEC Broadband Committee & State SPOC



Chief Mike Duyck
Committee Chair



Ben Gherezgiher
State SPOC



William Chapman
State SWIC



Oregon State Support Team



ENTERPRISE
information services

FirstNet in Oregon.



Any
questions?

“In theory there is no difference between theory and practice; in practice there is”

– Yogi Berra





ENTERPRISE

information services

Contact Information



Chief Mike Duyck

Chief (ret) and SIEC Chair
Broadband Committee Chair

e: Chief.duyck@gmail.com



Ben Gherezgiher

Assistant State Chief Information
Officer

State SPOC

e: Ben.GHEREZGIHER@oregon.gov

p: 503.586.6978



William Chapman

State SWIC

e: William.CHAPMAN@oregon.gov

Thank you for your time!