Handout to accompany:

OREGON ENERGY SECURITY PLAN MEETINGS

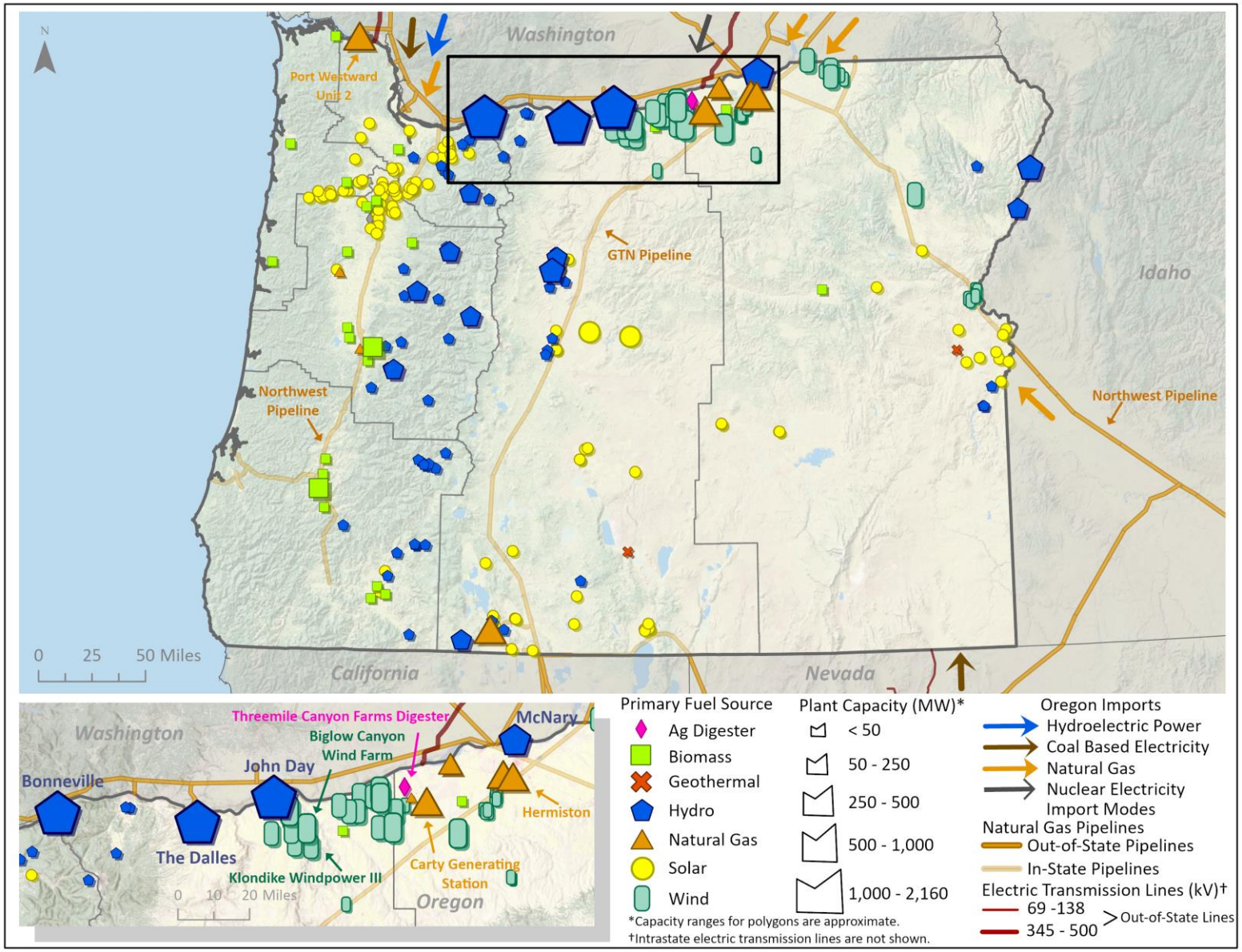
Deanna Henry
Tom Sicilia, RG
Max Woods
ODOE

Casey Steadman, PHD
Andrew Eiswerth
CNA

OREGON DEPARTMENT OF ENERGY

Electricity

Infrastructure – Sourcing

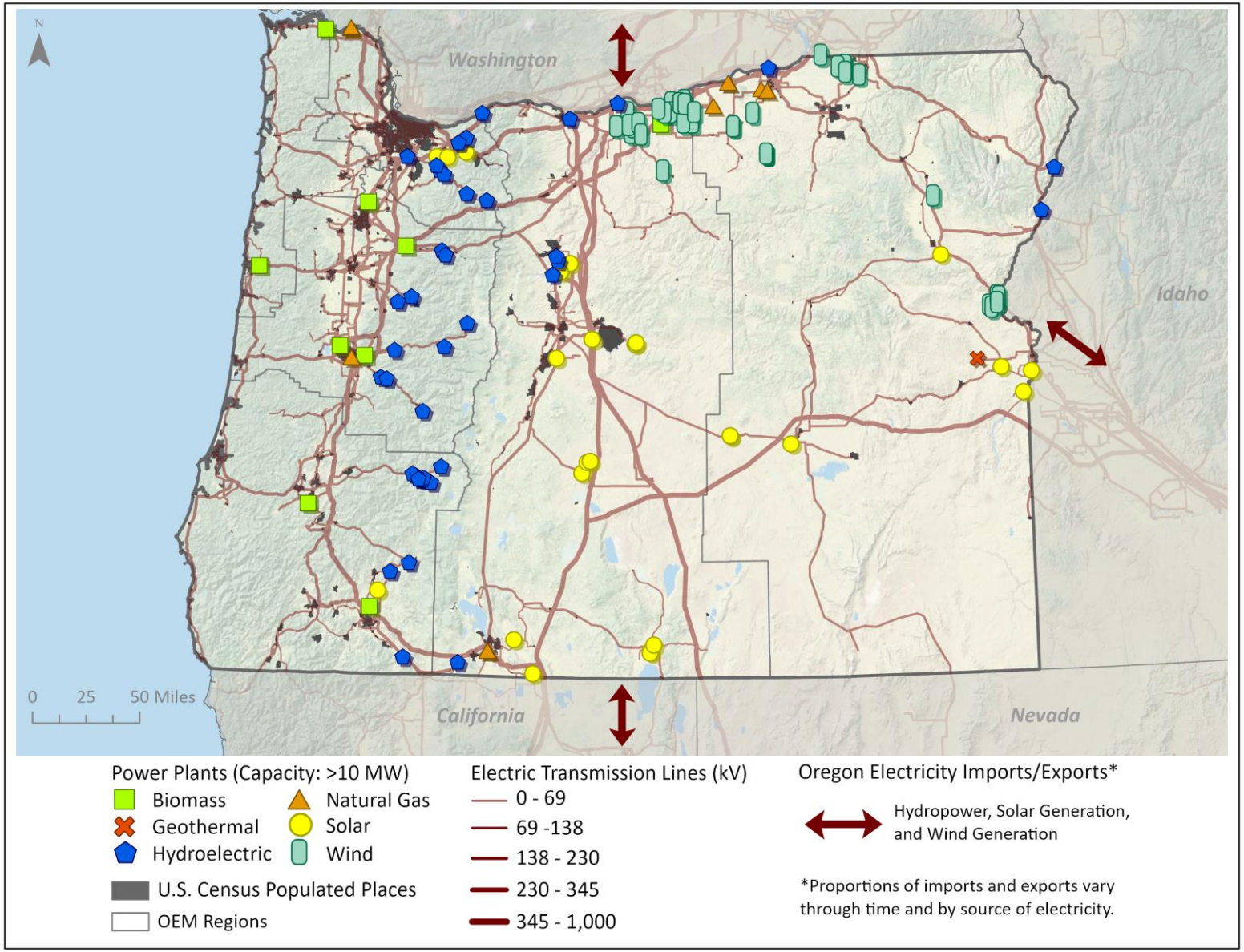


Data sources:

EPA eGRID
https://www.epa.gov/egrid/download-data
Homeland Infrastructure Foundation-Level Data
https://hifld-geoplatform.hub.arcgis.com/search?q=transmission%20lines
U.S. Energy Information Administration
https://atlas.eia.gov/datasets/4a158d2113f145039f71b80d07e2c19c_0/explore?location=44.487836%2C-119.613340%2C6.86

Electricity

Infrastructure – Transmission



Data sources:

EPA eGRID
https://www.epa.gov/egrid/download-data
Homeland Infrastructure Foundation-Level Data
https://hifld-geoplatform.hub.arcgis.com/search?q=transmission%20lines

OEM: Oregon Department of Emergency Management

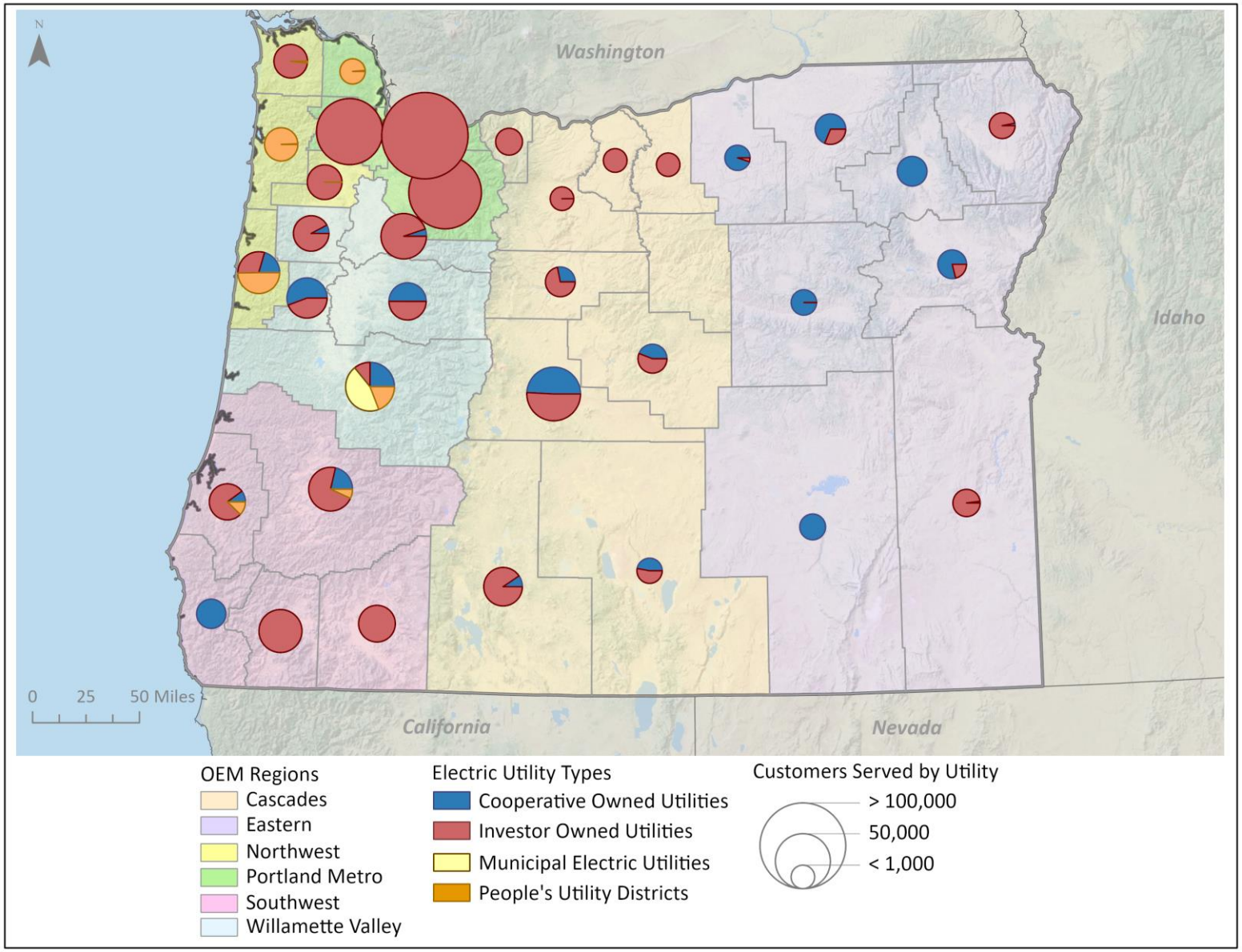
Electricity

Infrastructure – Customers

41 Total Utilities

3 Investor Owned Utilities

38 Other Utilities

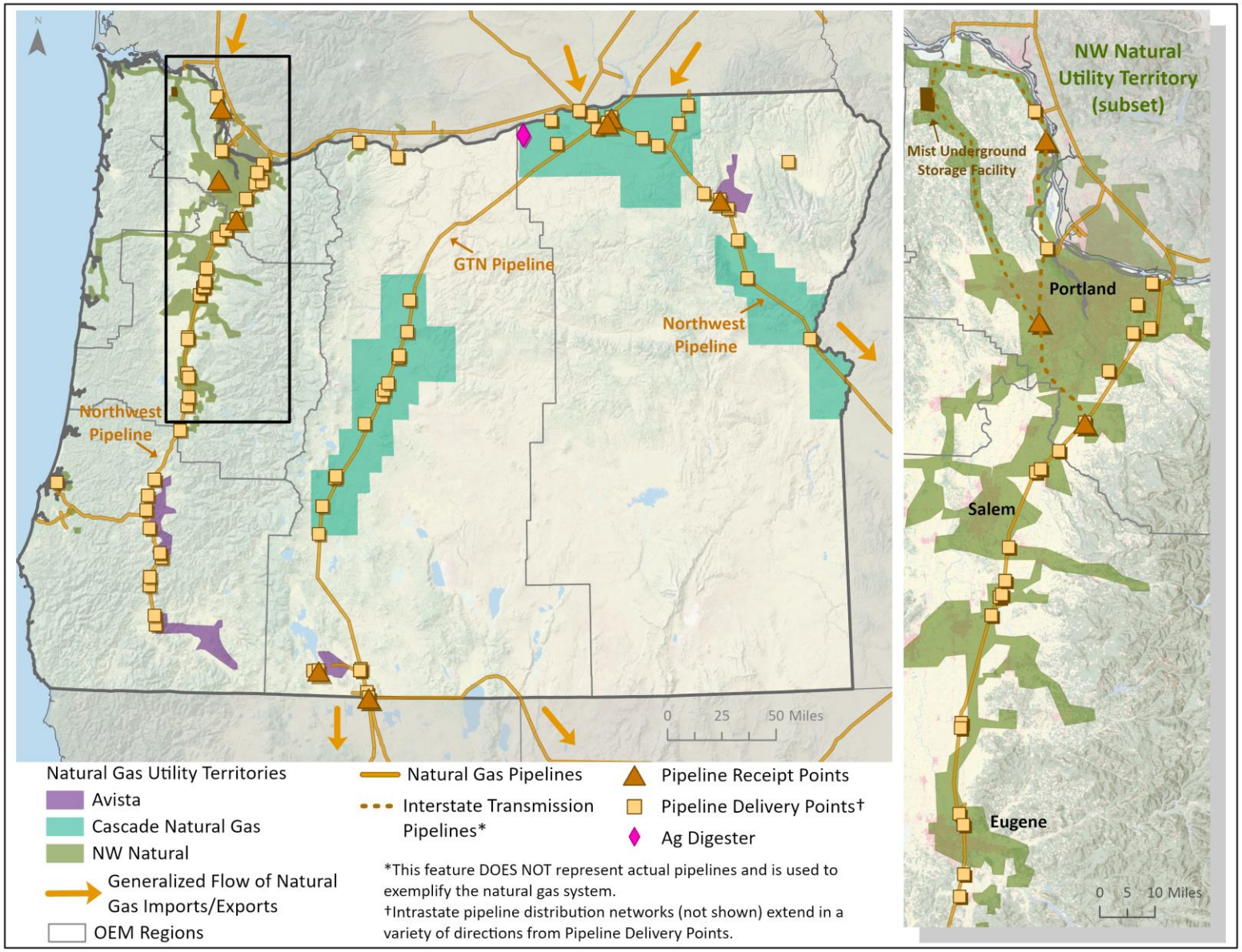


OEM: Oregon Department of Emergency Management

Data sources:
PowerOutage.us
https://poweroutage.us/

Natural Gas

Infrastructure



Data sources:
Homeland Infrastructure Foundation-Level Data
https://gii.dhs.gov/HIFLD
Oregon Public Utility Commission
https://www.oregon.gov/puc/utilities/Documents/MAP-GasCompany.pdf
U.S. Energy Information Administration
https://atlas.eia.gov/datasets/4a158d2113f145039f71b80d07e2c19c_0/explore?location=44.487836%2C-119.613340%2C6.86

OEM: Oregon Department of Emergency Management

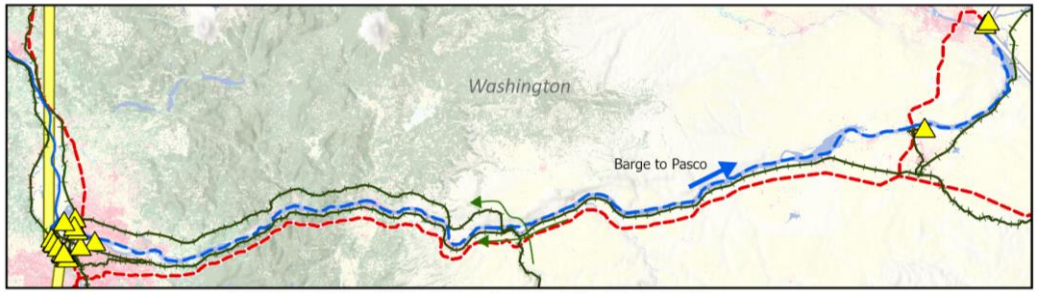
Liquid Fuels

Infrastructure – Diesel Sourcing

OREGON DEPARTMENT OF ENERGY

Diesel Fuel - Inbound Flow to Oregon

Columbia River



Rail and roads closely follow river. Map uses offsets for visibility.

Share by mode

(approximate - varies seasonally and year to year)

Marine	Rail	Truck	Pipeline
(barge)			(thru)
30	2	3	66

Flow routes

Inbound flow - percent on route

<5% 10% 30% 60%

Petroleum Terminals

Destination for most inbound flow

Counties

OEM Regions

Other States

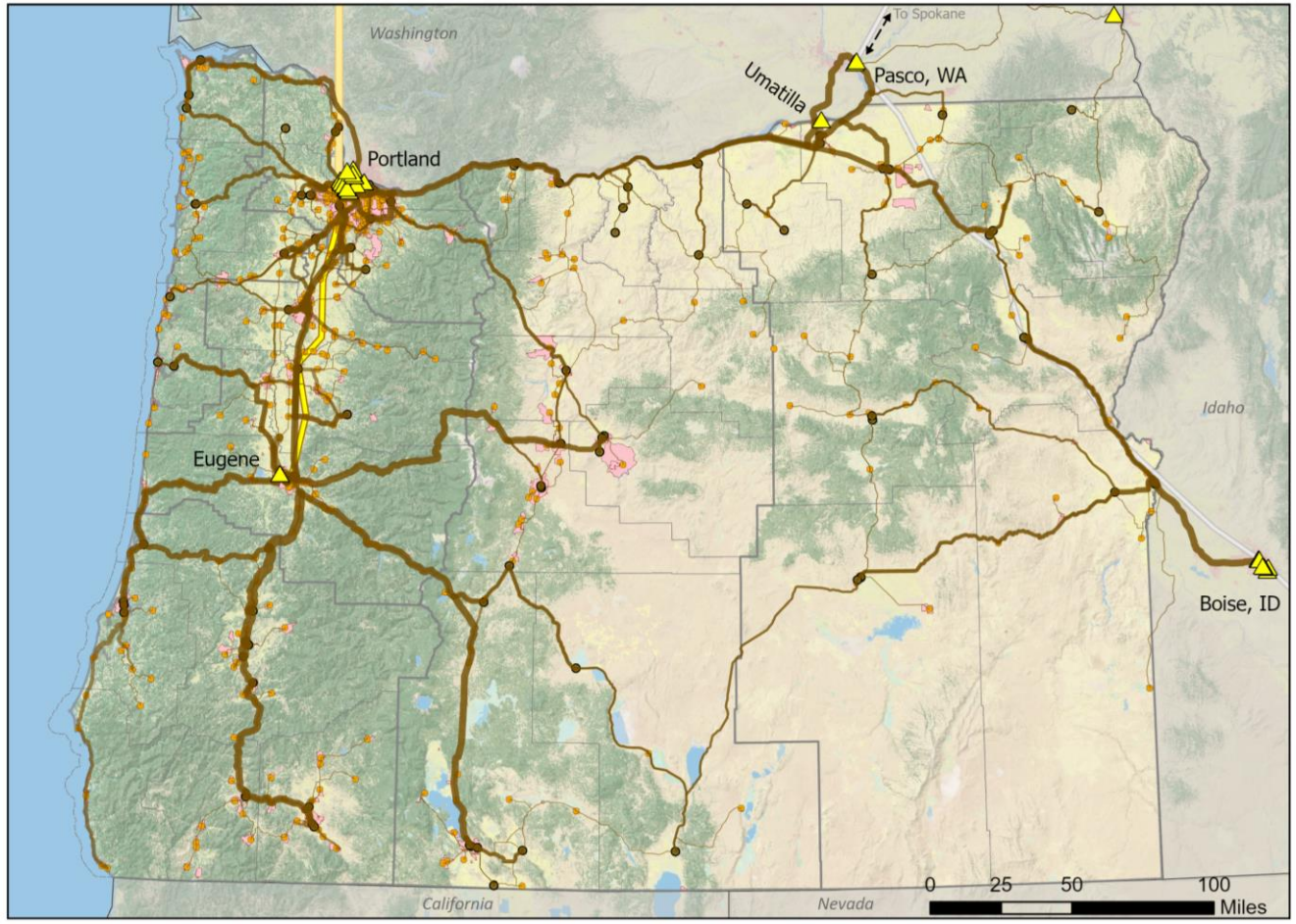
Data sources:
Homeland Infrastructure Foundation-Level Data (https://gii.dhs.gov/HIFLD)
Oregon Department of Emergency Management (https://oregon-oem-geo.hub.arcgis.com/)
Oregon Department of Energy
Oregon Department of Transportation

Liquid Fuels

Infrastructure – Diesel Distribution

Finished Diesel Flows within Oregon

Flow of finished diesel and biodiesel blends from terminals to fuel distributors and retailers/end users. Routes depict minimum trucking time and width of lines represents diesel and biodiesel capacity served.

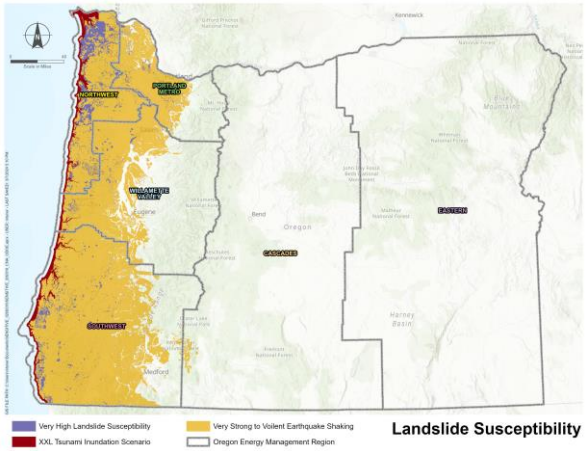


Data sources:
Homeland Infrastructure Foundation-Level Data
https://gii.dhs.gov/HIFLD
https://hifldgeoplatform.opendata.arcgis.com/datasets/aaa3767c7d2b41f69e7528f99cf2fb76_7/explore?location=45.957491%2C-119.794073%2C6.70
Oregon Department of Emergency Management
https://oregon-oem-geo.hub.arcgis.com/
Department of Energy Alternative Fuel Data Center
https://afdc.energy.gov/stations#/find/nearest
Oregon Department of Transportation
https://www.oregon.gov/odot/Data/Pages/GIS-Data.aspx#freight

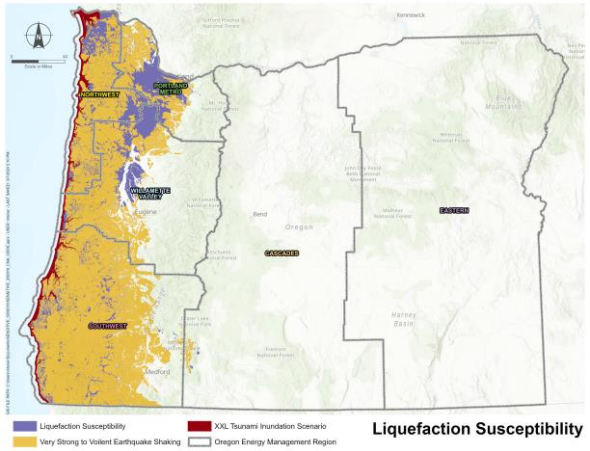
OEM: Oregon Department of Emergency Management

Risk Assessment

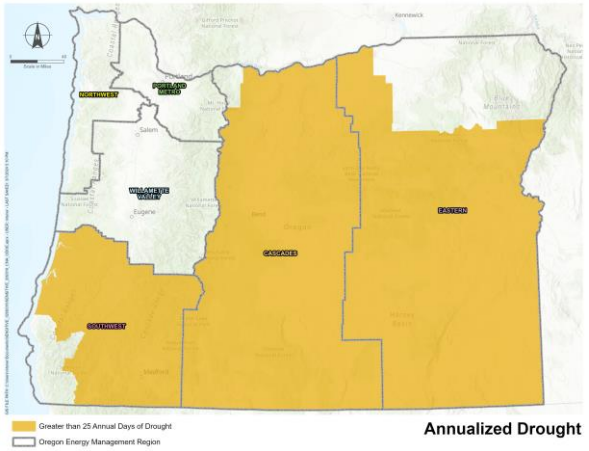
Natural Hazard Zones



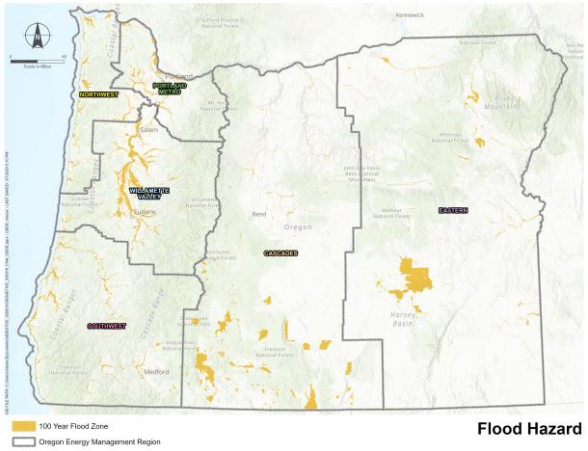
Landslide Susceptibility



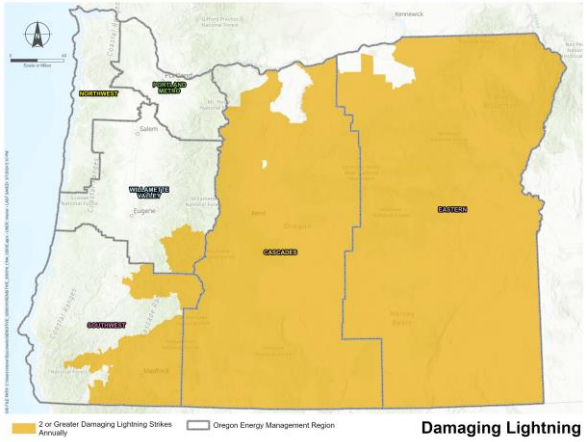
Liquefaction Susceptibility



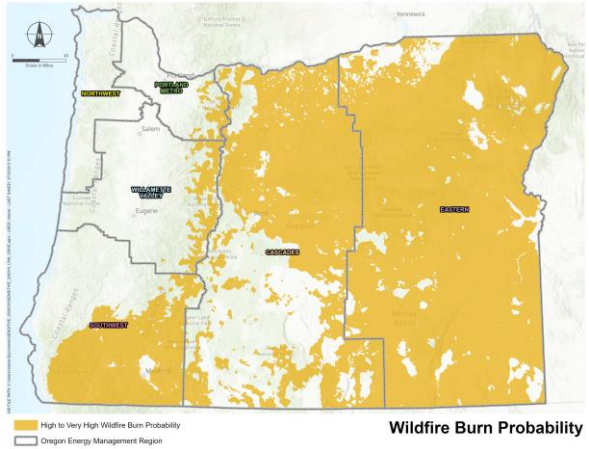
Annualized Drought



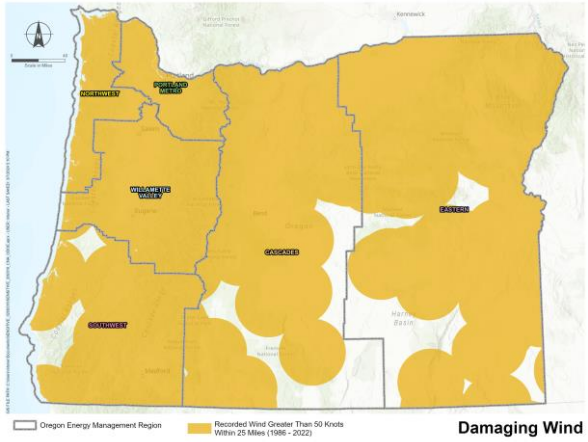
Flood Hazard



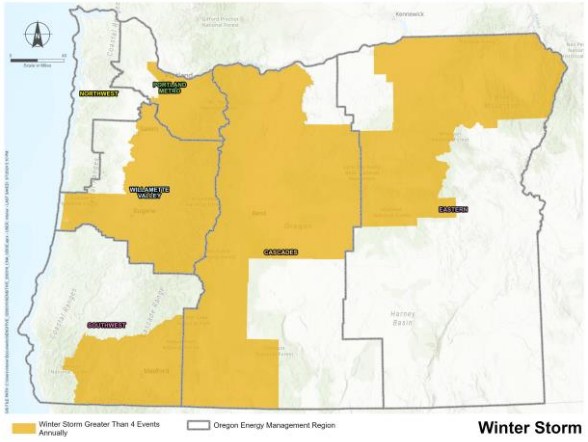
Damaging Lightning



Wildfire Burn Probability



Damaging Wind



Winter Storm

Electricity

Risk Assessment – Vulnerability Ranking

Overall Vulnerability Ranking

- Low (≤ 5)
- Moderate (6-8)
- High (≥ 9)

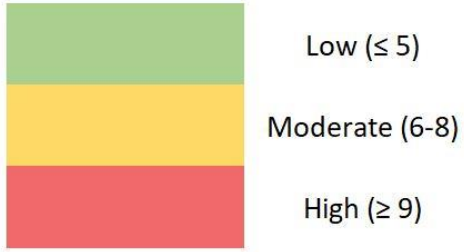
	Cascades	Eastern	Northwest	Portland Metro	Southwest	Willamette Valley
CSZ	4	5	5	5	6	4
Cyberattack	3	**2**	3	**2**	3	4
Drought	3	4	2	6	3	3
Flood	3	3	3	4	3	4
Lightning	5	4	2	4	3	3
Physical Attack	4	**2**	3	**2**	4	4
Wildfire	6	5	4	6	4	6
Wind Storm	6	6	5	6	6	6
Winter Storm	7	6	5	5	5	7

Underlined and bolded values indicates at least one response was unknown.

CSZ: Cascadia Subduction Zone Earthquake and Tsunami

Natural Gas

Risk Assessment – Vulnerability Ranking



	Cascades	Eastern	Northwest	Portland Metro	Southwest	Willamette Valley
CSZ	6	6	6	6	6	6
Cyberattack	2	3	2	2	3	2
Drought	N/A	N/A	N/A	N/A	N/A	N/A
Flood	4	4	4	4	4	4
Lightning	5	5	4	4	5	4
Physical Attack	4	4	7	7	4	6
Wildfire	5	5	5	5	6	5
Wind Storm	6	5	6	6	6	6
Winter Storm	4	4	4	4	4	4

N/A = no responses

CSZ: Cascadia Subduction Zone Earthquake and Tsunami

Liquid Fuels

Risk Assessment – Vulnerability Ranking

Overall Vulnerability Ranking

- Low (≤ 5)
- Moderate (6-8)
- High (≥ 9)

	Cascades	Eastern	Northwest	Portland Metro	Southwest	Willamette Valley
CSZ	5	6	7	7	7	7
Cyberattack	5	4	5	5	5	5
Drought	6	6	4	4	6	4
Flood	4	5	4	4	4	4
Lightning	7	8	6	6	7	6
Physical Attack	**3**	**3**	**3**	5	**3**	**3**
Wildfire	7	7	6	6	6	6
Wind Storm	7	8	7	7	7	7
Winter Storm	8	8	6	8	7	8

Underlined and bolded values indicates at least one response was unknown.

CSZ: Cascadia Subduction Zone Earthquake and Tsunami

Adaptive Capacity
Cyber Attacks

OREGON DEPARTMENT OF ENERGY

Category	Protective Measure Example
Identify	Develop an organizational understanding to manage risk to systems, assets, data, & capabilities
	Identify critical processes & assets
	Document information flows
	Maintain hardware & software inventory
	Establish policies for security that include roles & responsibilities
	Identify threats, vulnerabilities, & risk to assets
Protect	Develop & implement the appropriate safeguards to ensure delivery of services
	Manage access to information (e.g., unique accounts for each employee, restricted access to critical areas)
	Protect sensitive data (e.g., encryption while stored & transmitted; hard copies stored in secure areas)
	Conduct regular backups (e.g., backup frequently & store offline)
	Protect your devices (e.g., install host-based firewalls)
	Manage device vulnerabilities (e.g., update operating system & applications regularly)
	Train users (e.g., provide frequent training on policies, procedures, roles, & responsibilities)
Detect	Develop & implement appropriate activities to identify occurrence of a security event
	Test & update processes for detecting unauthorized entities & actions on networks
	Maintain & monitor logs to identify anomalies (e.g., changes to systems or accounts)
	Know expected data flows in order to identify the unexpected (e.g., information exported from internal database & exiting network)
	Understand the impact of security events
Respond	Develop & implement appropriate activities to take action regarding a detected security event
	Ensure response plans are tested
	Ensure response plans are updated
	Coordinate with internal & external stakeholders
Recover	Develop & implement appropriate activities to maintain plans for resilience & to restore any capabilities or services that were impaired due to a security event
	Communicate with internal & external stakeholders - account for what, how, & when information will be shared with various stakeholders
	Manage public relations & company reputation

Adaptive Capacity
Physical Attacks

OREGON DEPARTMENT OF ENERGY

Category	Protective Measure Example
Identify	Develop an organizational understanding to manage risk to systems, assets, data, & capabilities
	Identify critical processes & assets
	Document personnel activities
	Maintain asset inventory
	Establish policies for security that include roles & responsibilities
	Identify threats, vulnerabilities, & risk to assets
Protect	Develop & implement the appropriate safeguards to ensure delivery of services
	Manage access to assets (e.g., restricted access to critical areas)
	Protect your assets (e.g., physical barriers)
	Manage asset vulnerabilities (e.g., replace broken physical barriers)
	Train users (e.g., provide frequent training on policies, procedures, roles, & responsibilities)
Detect	Develop & implement appropriate activities to identify occurrence of a security event
	Test & update processes for detecting unauthorized entities in the physical environment
	Maintain & monitor logs to identify anomalies
	Know expected personnel activities in order to identify the unexpected
	Understand the impact of security events
Respond	Develop & implement appropriate activities to take action regarding a detected security event
	Ensure response plans are tested
	Ensure response plans are updated
	Coordinate with internal & external stakeholders
Recover	Develop & implement appropriate activities to maintain plans for resilience & to restore any capabilities or services that were impaired due to a security event
	Communicate with internal & external stakeholders - account for what, how, & when information will be shared with various stakeholders
	Manage public relations & company reputation

Adaptive Capacity
Natural Hazards

PHYSICAL		OPERATIONAL	
Measure	**Protective Measure Example**	**Measure**	**Protective Measure Description**
Harden	Install barriers and shields (e.g., flood barriers around substations) Design structures with earthquake-resistant materials Use fire-resistant construction materials	COOP Continuity of Operations Plan	Ensures organizations are able to continue performing essential functions under distinct circumstances
Redundancy	Implement backup power systems (e.g., generators) Install multiple fuel supply lines Integrate access to alternate reservoirs	EOP Emergency Operation Plan	Assigns responsibilities to individuals and determines how actions will be coordinated internally and externally under distinct circumstances
Remove	Shift critical infrastructure outside of flood and hazard areas	ERP Emergency Response Plan	Lays out the series of steps an organization will take under distinct circumstances
Upgrade	Enhance cooling systems for higher temperatures Increase efficiency of drainage systems	ISP Integrity Safety Plan	Assesses and mitigates risks in order to reduce the likelihood and consequences of distinct incidents
Weatherize	Adopt freeze prevention measures (e.g., pipe insulation) Apply hail-resistant coatings Cover and protect outdoor machinery Install storm windows	SitAw Situational Awareness	Improves the ability to perceive, understand, and effectively respond to distinct circumstances