Avangrid
A member of the
Iberdrola Group

Operational Technology (OT) Cybersecurity in Electricity Generation

October 4, 2023

What to learn

- What the electricity grid looks like to a generator based in Oregon.
- Regulatory compliance: Where doing the minimum is not enough.
- What it looks like to lose electricity due to a cyber event.
- Cybersecurity as an insurance policy.

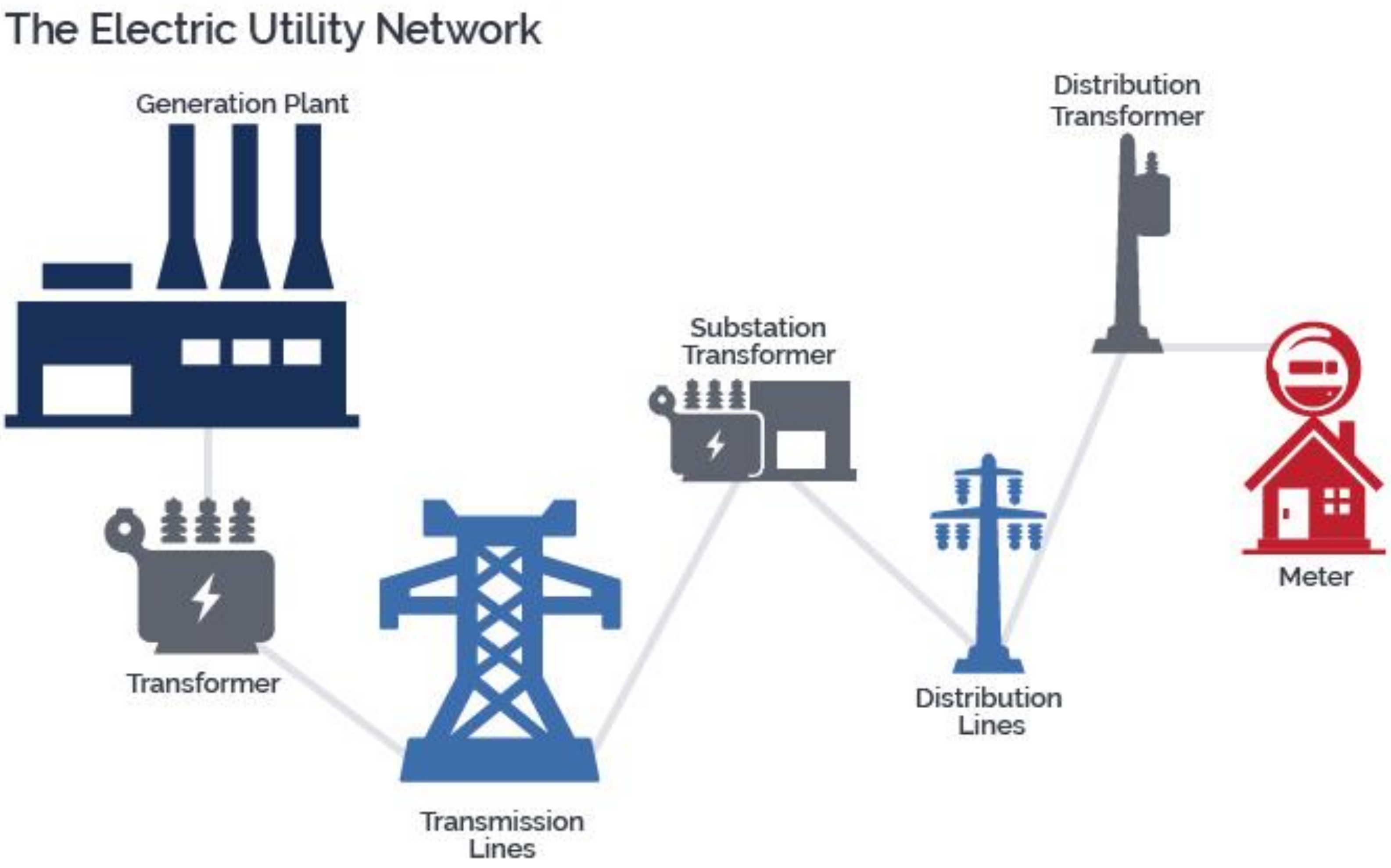
Why it matters

Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," identifies 16 critical infrastructure sectors. Within that group of 16 sectors, the energy sector plays an important role.

The directive, "identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors."

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems

The Grid



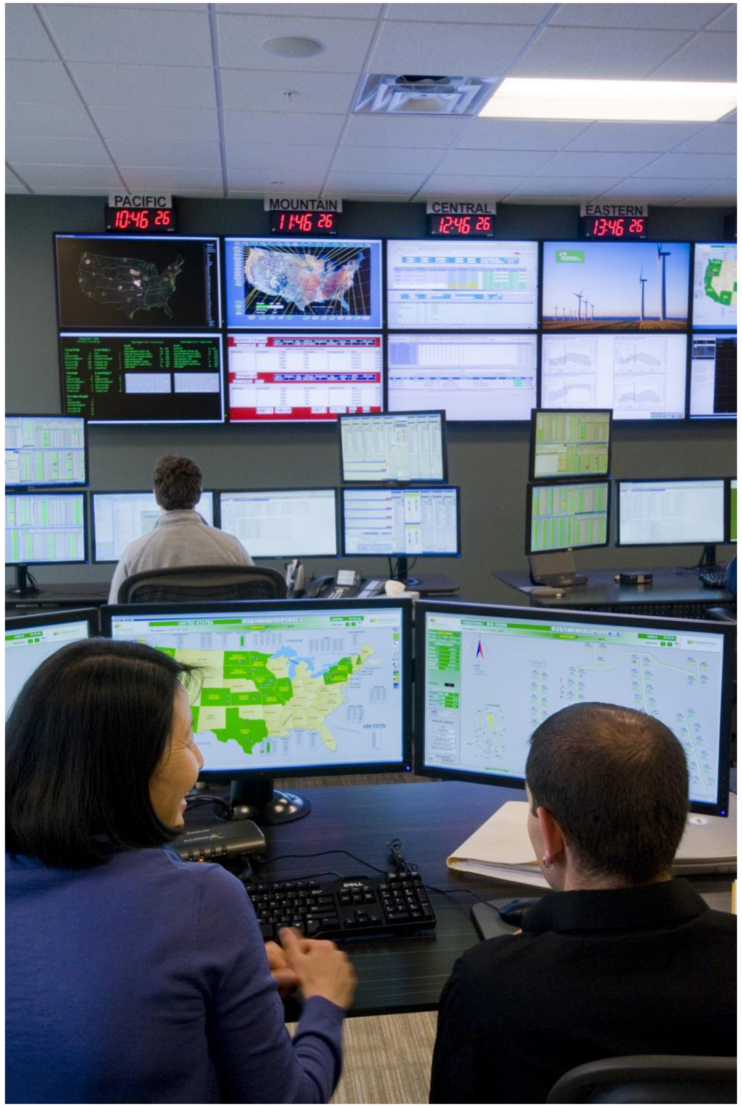
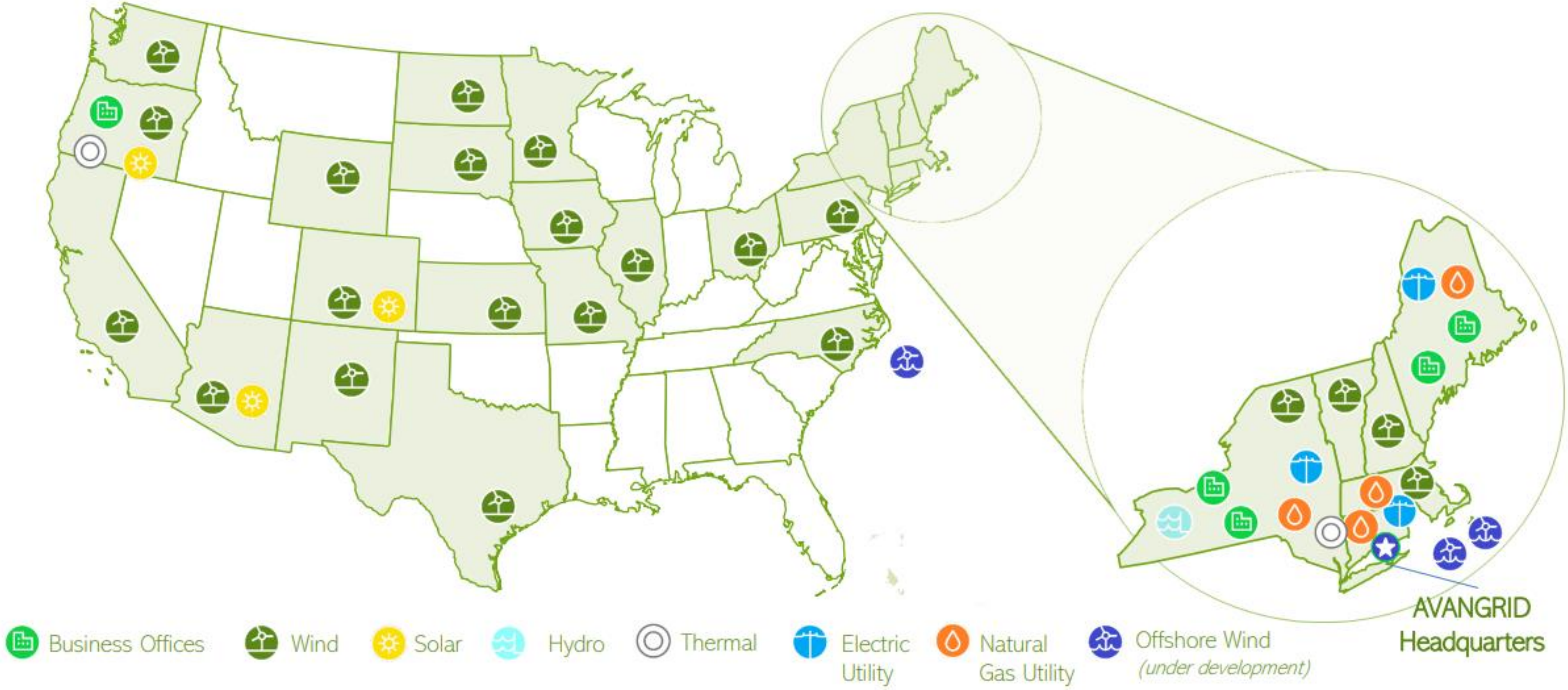
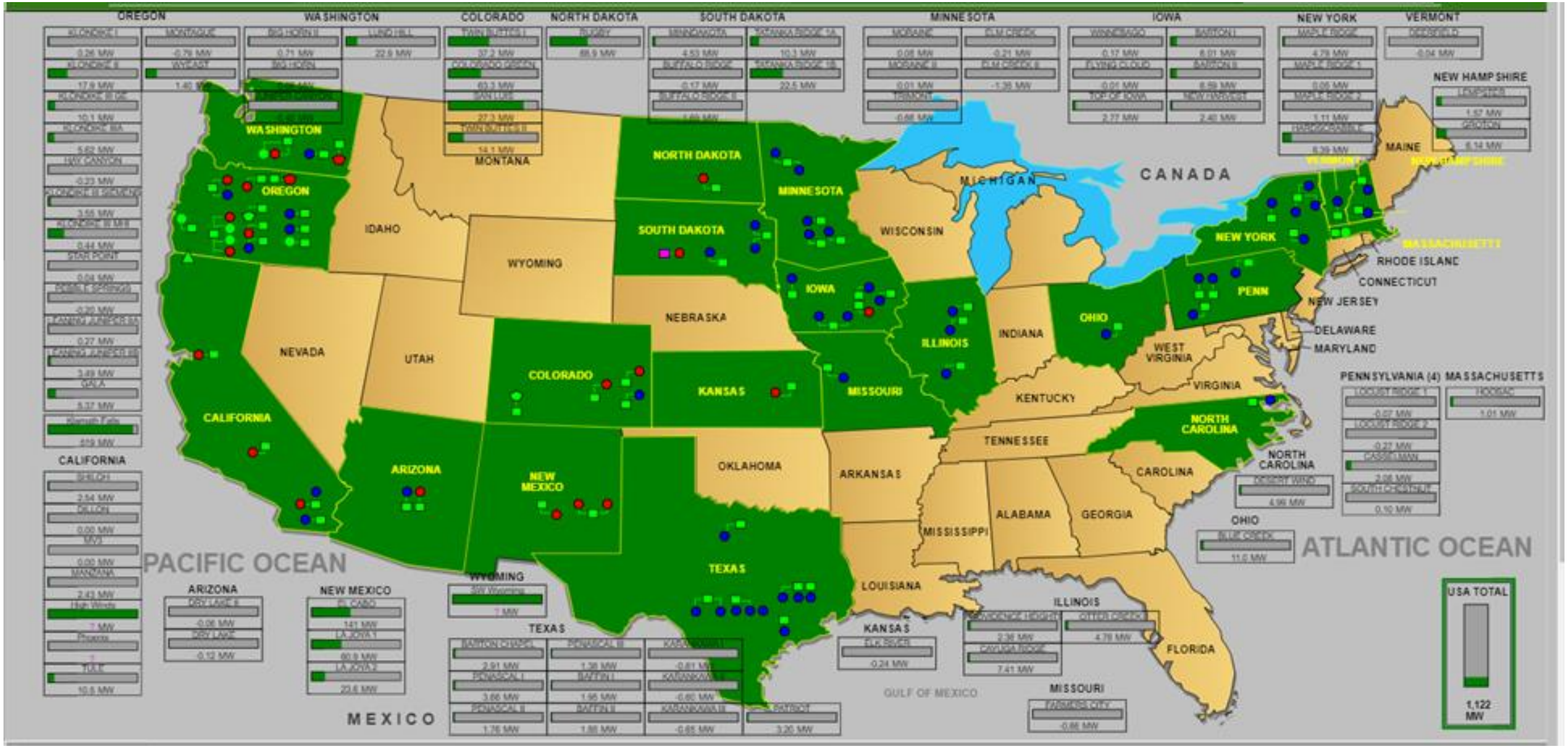


Image courtesy of American Public Power Association

Avangrid


AVANGRID Headquarters
Business Offices
Wind
Solar
Hydro
Thermal
Electric Utility
Natural Gas Utility
Offshore Wind
(under development)

Avangrid sites controlled from Oregon



~82 sites, 22 states, nearly 9000 MW of installed capacity

The Western Interconnection

- **136,000 miles of transmission line.**

- **Electricity travels longer distances than in the east.**

- **In spring and summer, with demand low in the PNW, excess power moves to California.**

- **With a large attack surface, power is continuously susceptible to cyber, physical, and natural events.**

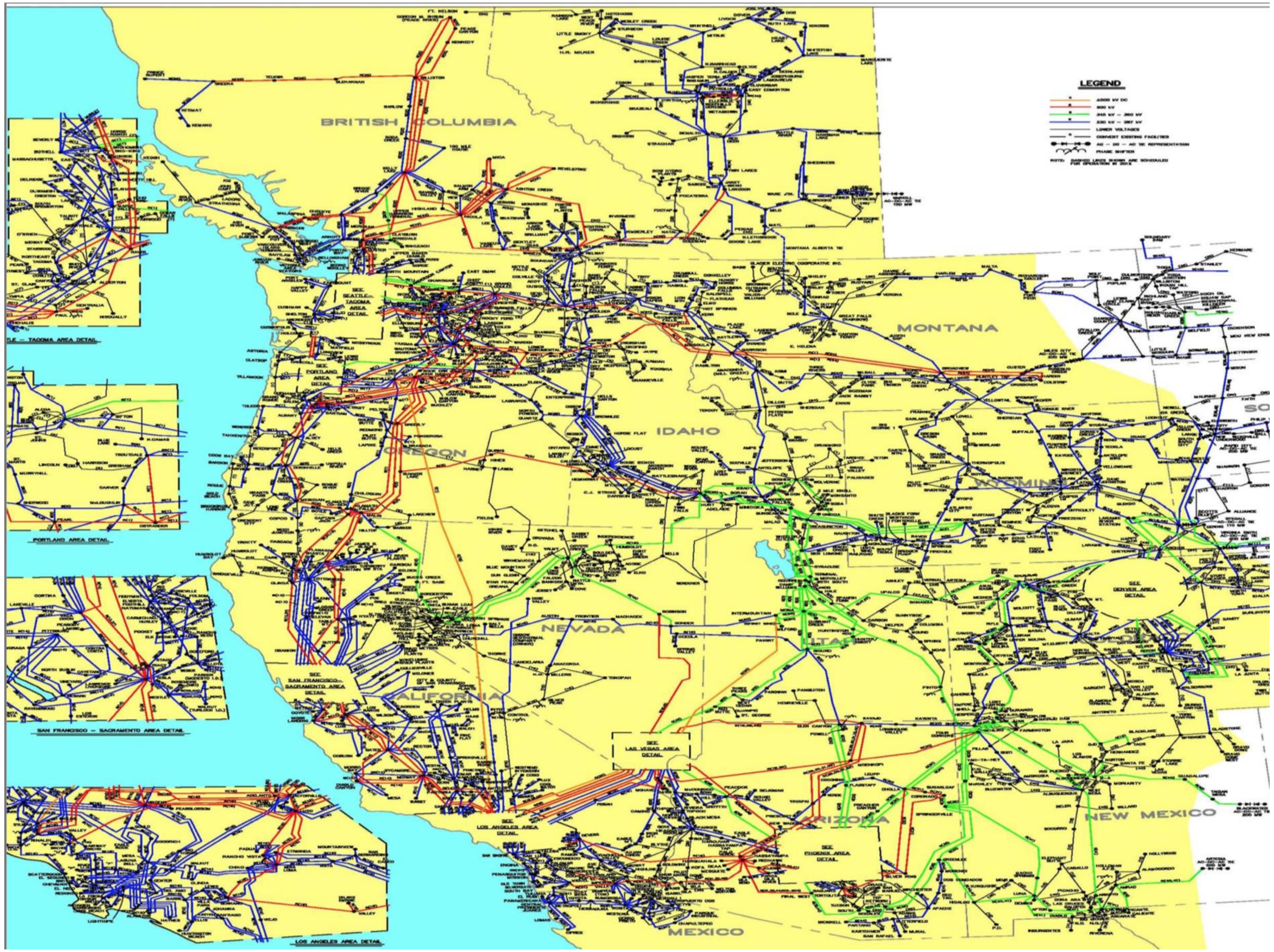


Image courtesy of Western Electricity Coordinating Council (WECC)

Compliance as a baseline

North American Electric Reliability Corporation, Critical Infrastructure Protection (NERC CIP)

- Set of requirements designed to secure the assets required for operating North America's bulk electric system.

- Designed for every electricity provider from small rural to multinational.

- Substantially stronger than other countries but that may not be saying much.

- Federal government adjusting but going to take time.

Image courtesy of Waylon Joseph Smithers, Jr./Springfield Nuclear Power Plant (SNPP)

When the lights don’t turn on

Avenues of approach

- University of Tulsa research in 2017.
  - On-site vs. remote access
- Nation state vs. organized crime vs. disgruntled employee vs. vandalism
- What is intent? Does it matter?
  - Wide-spread destruction to psychological manipulation
  - Money, damage, gain strategic advantage

Image courtesy of Kristian Hoyle/Wales News Service

When the lights don’t turn on

Defense and Recovery

- **How much risk is your organization willing to accept?**
  - **Money**
  - **Image**

- **Where do you put your limited resources?**
  - **People**
  - **Tools**
  - **Services**

- **The ability to recover to pre-event conditions**

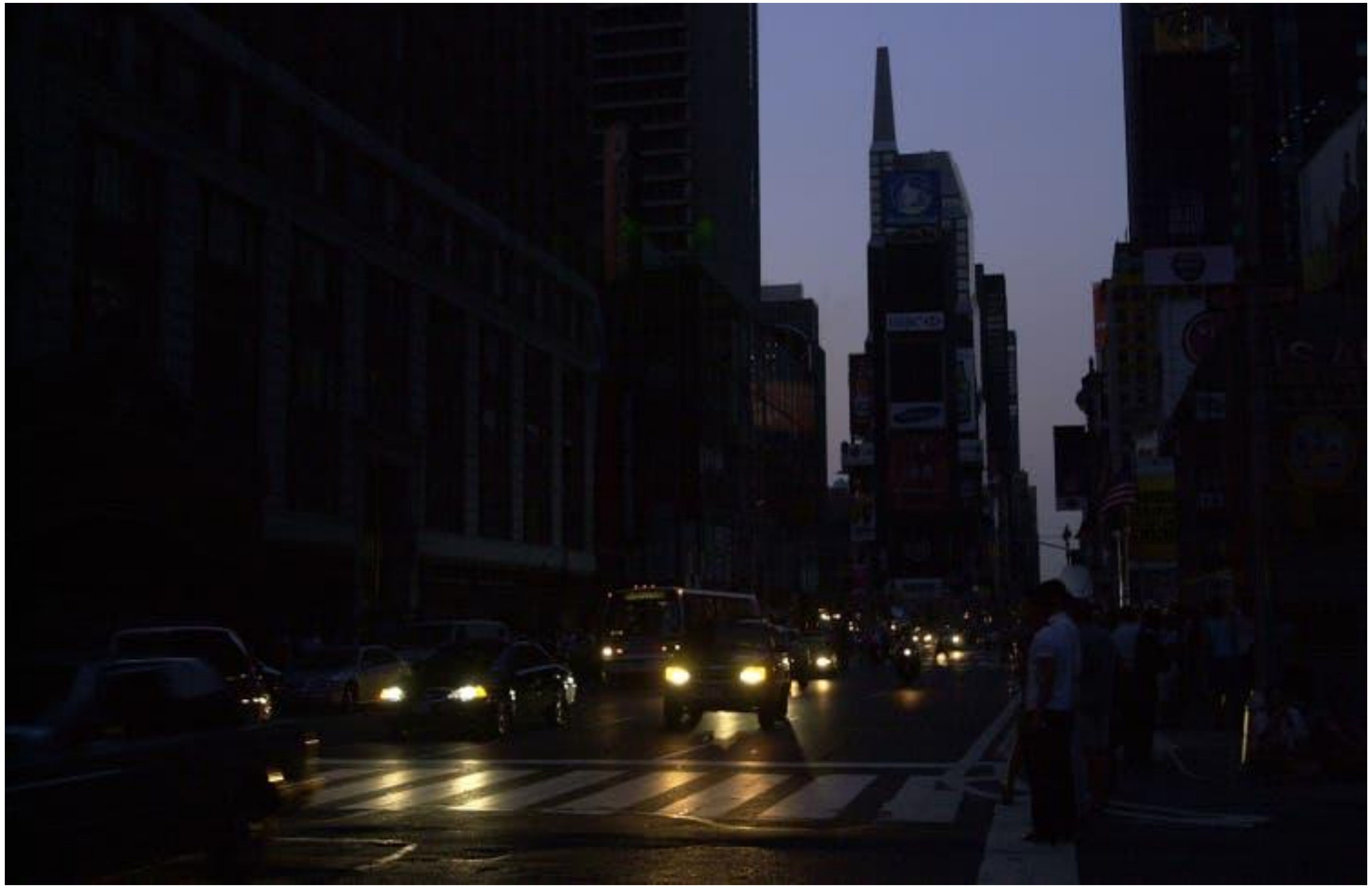


Image courtesy of Robert Rosamilio/NY Daily News/Getty Image

Cybersecurity as an insurance policy

Avangrid
A member of the Iberdrola Group

Selling the idea to leadership

- Determining cost of failure
  - Summer & Winter dynamics
  - NERC or SEC penalties
  - Damaged equipment
- What is your organizations image worth?
  - Is a PR firm less expensive than a strong cyber program?
- Is regularity of events hurting security practitioners?

Avangrid

A member of the
Iberdrola Group