NARUC

Serving the consumer interest by seeking to improve the quality and effectiveness of public utility regulation in America.

Cyber security and the Actions Regulators Need to Take

Commissioner Philip Jones, President, NARUC;
Commissioner, Washington Utilities and Transportation Commission

10th EU-US Energy Regulators Roundtable
April 8-9, 2013

Setting the Stage

- **Newspapers, Internet filled with stories about breached security**
  - **Banks, credit card companies, federal agencies**
  - **No utilities--yet**
- **BUT--40% of cyber attack attempts in 2012 were on energy facilities**
- **Congress, Administration, State Action**
  - **Everyone has a role to play—communication, participation between public and private entities a necessity**

NARUC Activities

- **Grants and Research Department**
  - **Cybersecurity for State Regulators, available on NARUC Website**
  - **Training sessions—26 States by the end of May 2013!**
- **Critical Infrastructure Committee**
- **Themes—Ask Questions, Be Proactive**
  - **Utility regulators don't need to be IT experts**
  - **Ask questions: Utility planning, IT-procurement, standards, personnel policies**
  - **Determine what is a wise investment, what isn't**

Washington Action

- **White House Executive Order**
  - **Released in February 2013**
  - **Promotes information sharing between federal agencies, encourages industry participation**
- **Congress**
  - **House, Senate offer different proposals**
    - **In 2012, House-passed bill focused on voluntary framework, Senate wanted more top-down approach, did not act**
    - **NARUC sympathetic to House approach**
  - **House Committees planning April "Cyber Week" to focus on legislation**
  - **Passage unclear, despite support for legislation from Congress and White House**

Threats, Vulnerabilities

- **Imminent Threat**
  - **Impending threat to security, safety of the grid**
  - **Feds can/should act to preserve the grid at all levels**
    - **Timing is everything**

- **Vulnerabilities**
  - **Weaknesses on the grid requiring less immediate attention**
  - **Utilities own, operate the network; they should already have a plan for dealing with weaknesses**
  - **What might be necessary in Washington, D.C., likely not necessary in Seattle, Washington**

Need for Communications

- **Federal intelligence agencies have more information**
- **Information must be shared with utilities, so they can act and shore up their systems**
- **Confidentiality**
  - **States can establish critical infrastructure information policies governing public-data requests**
  - **Sept. 11, 2001, other national security events: We've dealt with confidentiality before**

Understanding the Risks

- **U.S. Rep Mike Rogers, Chair, House Intelligence Committee**
  - **"If your CIOs tell you they've got this all figured out, I suggest you get yourself a new CIO"**
- **Cyber threat real, dynamic, constantly evolving**
  - **We may never solve it**
- **But it is not unmanageable**

Understanding the Risks

- **All utility infrastructure is vulnerable**
  - **Mother Nature—hurricanes, tornados, reckless drivers, age**
- **We manage these risks everyday**
  - **Lights stay on, but grid remains as vulnerable as ever**
- **Stakes are higher**
  - **Utilizing risk-management approach for cyber protection is essential**
- **Communication is key**
  - **Public, private partnership essential**

Questions?

- Questions?