Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Cyber Security Implications of Synchrophasor Applications

March 27, 2014

Jeff Dagle, PE
Chief Electrical Engineer and Team Lead
Electricity Infrastructure / Transmission System Resilience
Pacific Northwest National Laboratory
(509) 375-3629
jeff.dagle@pnnl.gov

Security of Synchrophasors

- Synchrophasors are becoming part of the bulk electric system and will require physical and cyber security
  - ***But these systems shouldn't be treated any differently than other forms of measurement and control telemetry***
- Synchrophasor systems will coexist with other bulk electricity system (BES) cyber infrastructure and will have similar dependencies on common communications and network elements
- System designers and owners are leveraging emerging cyber-security standards and technologies
- Currently available phasor applications require further data analysis, software refinement and operational validation to be fully effective; many are in advanced development and testing and are not in full operational use
  - Therefore, many of these systems are not currently considered critical cyber assets
- Due to nature of continuous, high-volume data flows, new technology will likely be required for measurement, communications, and applications
  - Technology anticipated to undergo rapid change and refinement over the next several years that is being addressed by ongoing research programs