Update:
DOE's Grid Modernization Initiative

NARUC Staff Subcommittee on Critical Infrastructure

February 14, 2016

David Meyer, Senior Advisor
DOE Office of Electricity Delivery
and Energy Reliability

GMI Will Have National Impact -- 88 projects, $220 Million

Drivers of Change

- Changing Electricity Supply Mix
- Threats to Resilience and Reliability
- New Market Opportunities for Consumers
- Information and Control Technologies
- Aging Infrastructure

DOE Multi-Year Plan

- Devices and Integrated Systems
- Sensing and Measurement
- System Operations and Control
- Design and Planning Tools
- Security and Resilience
- Institutional Support

Regional Demonstrations

- Low Reserve Margin Demos
- Clean Distribution Feeders
- Grid Analytics Platform

Modernized Grid

**Goal:
Power the U.S. economy for the 21st Century**

Grid Modernization Lab Call: Proposed Pioneer Partnerships
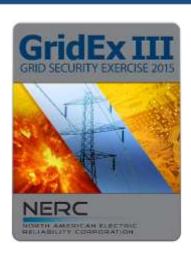
For more information …

- **See 2-page handout provided**

- **Go to: http://energy.gov/doe-grid-modernization-laboratory-consortium-gmlc-awards**
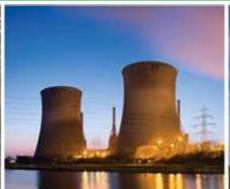
- **Contact: David.Meyer@hq.doe.gov**

E-ISAC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

GridEx III

1 Exercise crisis response and recovery

2 Improve communication

3 Identify lessons learned

4 Engage senior leadership

Cyber Supply Chain Risk Management References

- ***Cybersecurity Procurement Language for Energy Delivery Systems***
  http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

- ***Cybersecurity Capability Maturity Model (C2M2)*** http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

- ***FERC Supply Chain Technical Conference statements***:
  http://www.ferc.gov/CalendarFiles/20151223134159-RM15-14-000-Agenda.pdf

- ***Utilities Telecom Council (UTC) Cyber Supply Chain Risk Management for Utilities—Roadmap for Implementation*** http://www.utc.org/sites/default/files/public/UTC_Public_files/SupplyChain2015.pdf

- **NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations** http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

- **NIST Cyber Supply Chain resources** http://csrc.nist.gov/scrm

- ***ISO/IEC 27036, Information Security for Supplier Relationships***
  http://www.iso.org/iso/search.htm?qt=27036&sort_by=rel&type=simple&published=on&active_tab=standards

- ***ISO/IEC 20243, Open Trusted Technology ProviderTM Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products***
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67394

- ***IEC 62443-2-4, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*** https://webstore.iec.ch/publication/22810

- ***National Electrical Manufacturers Association (NEMA) Supply Chain Best Practices***
  https://www.nema.org/news/Pages/NEMAs-Cybersecurity-Council-Releases-Supply-Chain-Best-Practices.aspx