## Smart Grid Task Force
### Meeting Agenda

June 23, 2011 | 8:30 AM – 3:30 PM

NERC Atlanta Office  
3353 Peachtree Road NE  
Suite 600 North Tower  
Atlanta, GA 30326

### Agenda

**Smart Grid Task Force**  
**Thursday, June 23, 2011**

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Leader</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 am</td>
<td>1. Administrative Matters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Welcome and Introductions</td>
<td>Paul McCurley, NRECA</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>b. Antitrust Guidelines</td>
<td>Eric Rollison, NERC</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>c. Meeting Logistics and Arrangements</td>
<td>Eric Rollison, NERC</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>d. Agenda Review</td>
<td>Paul McCurley and Eric Rollison</td>
<td>Information</td>
</tr>
<tr>
<td>8:45 am</td>
<td>2. NERC and its Role in the Electricity Industry (NERC 101)</td>
<td>Eric Rollison, NERC</td>
<td>Information</td>
</tr>
<tr>
<td>9:15 am</td>
<td>3. Critical Infrastructure Coordinated Strategic Action Plan</td>
<td>Eric Rollison, NERC</td>
<td>Discussion</td>
</tr>
<tr>
<td>9:45 am</td>
<td>4. NERC Smart Grid Task Force Objectives and Deliverables</td>
<td>John Moura, NERC</td>
<td>Discussion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paul McCurley, NRECA</td>
<td></td>
</tr>
<tr>
<td>10:30 am</td>
<td><strong>Break</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:45 am</td>
<td>5. Smart Grid Work Plan and Subgroup Leadership</td>
<td>Paul McCurley, NRECA</td>
<td>Information</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td>Presenters</td>
<td>Notes</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>11:00 am</td>
<td>6. Panel: SGTF Vice Chairs Review of Challenges of First Paper</td>
<td>Vice Chairs of SGTF</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>a. Characteristics – Virginia Whitiker</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Cyber Security – Sandy Bacik</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Planning and Operations – Paul Myrda</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Research and Development – Maria Illic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00 pm</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30 pm</td>
<td>7. Subgroup Breakout Meetings</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>2:30 pm</td>
<td>Break from Subgroup Meetings and Return to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:45 pm</td>
<td>8. Subgroup Reports</td>
<td>All</td>
<td>Discussion</td>
</tr>
<tr>
<td>3:15 pm</td>
<td>9. Meeting Schedule for 2011</td>
<td>Eric Rollison, NERC</td>
<td>Information</td>
</tr>
<tr>
<td>3:25 pm</td>
<td>10. Review of Action Items and Next Steps</td>
<td>Paul McCurley, Eric</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rollison and John Moura</td>
<td></td>
</tr>
<tr>
<td>3:30 pm</td>
<td>11. Adjourn</td>
<td>All</td>
<td>Information</td>
</tr>
</tbody>
</table>
The North American Bulk Power System: A Reliable Future

Eric Rollison

Engineer of Reliability Assessments
About NERC: Mission

To ensure the reliability of the North American bulk power system

- Develop and enforce reliability standards
- Assess current and future reliability
- Analyze system events and recommend improved practices
- Encourage active participation by all stakeholders
- Pursue mandatory standards in all areas of the interconnection
Energy Policy Act of 2005

  - Electric Reliability Organization that would span North America
  - FERC oversight in the U.S.
- The legislation stated that compliance with reliability standards would be mandatory and enforceable.
NERC Reliability Assessments

- Peak Demand Forecasts
- Resource Adequacy
- Transmission Adequacy
- Key Issues & Emerging Trends Impacting Reliability
- Regional Self-Assessment
- Ad-hoc Special Assessments
Reliability Risk Management Concepts

Cornerstone of risk-management concepts

Severity

Avoid

High Impact
Low Frequency
(including CIP)

Learn and Reduce

Inverse
Cost-Benefit

Reporting Threshold

Frequency
Transmission Growth at a Glance
Transmission Growth at a Glance
Transmission Growth at a Glance
Transmission Growth at a Glance
Transmission Growth at a Glance

2010

[Map of the United States showing transmission lines]
One HUGE Machine
Basic Elements
Bulk Power System Designed to Meet Demand in Real Time

Typical Daily Demand Curve

- **Base Load**
- **Intermediate Load**
- **Peak Load**

**Operating Reserves**

**Energy:**
Electricity Produced over Time

**Capacity:**
Instantaneous measure of electricity available at peak
Brutal Facts

- Stuff will happen
  - Things blow up
  - People make mistakes
  - The only thing you know about your load forecast is that it is wrong

- You don’t know when stuff will happen
- You don’t have enough money to keep stuff from happening
- The wind doesn’t always blow (…and its not free)
- Uncertainty is the worst!
Smart Grid and Cyber Security
Smart Grid – Everybody has a vision...
Reduce electric sector greenhouse gas emissions;
Enable consumers to better manage and control their energy use and costs;
Improve energy efficiency, demand response, and conservation measures;
Interconnect renewable energy resources;
Improve bulk power and distribution system reliability;
Manage energy security; and
Provide a platform for innovation and job creation.
Key Findings of the Smart Grid Report

Government initiatives and regulations promoting smart grid development and integration must consider bulk power system reliability implications.

Integration of smart grid requires development of new tools and analysis techniques to support planning and operations.

Smart grid devices and systems will change the character of the distribution system, potentially affecting bulk power system reliability.

Cyber security and control systems require enhancement to ensure reliability.

Research and development (R&D) has a vital role in successful smart grid integration.
As we look to the future, new resources like rooftop solar panels, large-scale wind generation, PHEV’s, and storage will bring unique characteristics to the grid that must be understood and effectively managed to ensure reliable and cost-effective deployment.

These new resources will be highly interdependent. Operational variability of large-scale wind generation can be effectively balanced by flexible resources like demand response, plug-in hybrids, and energy storage. Distributed variable generation will rely on conventional generation to ensure ancillary services and voltage and reactive support are available to maintain power quality.

The development and successful integration of these resources will require the industry to break down traditional boundaries and take a holistic view of the system with reliability at its core.
The “Smart Grid” completes the picture of a fully integrated system without boundaries. Stretching from synchro-phasors on the transmission system to smart appliances in the home, these systems will enable the visualization and control needed to maintain operational reliability.
Common Challenges

Cyber security is one of the most important concerns for the 21st century grid and must be central to policy and strategy. The potential for an attacker to access the system extends from meter to generator.
Building the 21st century grid requires a comprehensive and coordinated approach to policy and resource development – looking at the grid as a whole, not as component parts.
Electric Power: Players, Drivers, Etc.
Smart Grid Vision

- Reduce electric sector greenhouse gas emissions;
- Enable consumers to better manage and control their energy use and costs;
- Improve energy efficiency, demand response, and conservation measures;
- Interconnect renewable energy resources;
- Improve bulk power and distribution system reliability;
- Manage energy security; and
- Provide a platform for innovation and job creation.
The Smart Grid Landscape: Devices & Systems

NOTE: Placement of items in the plane above is for concept discussion purposes.
NERC’s Reliability Standards apply to all users, owners, and operators of the bulk power system and typically apply to facilities at the transmission and generation level.
Smart Grid may provide both system benefits and reliability considerations to the distribution system and bulk power system.
The aggregate impacts of Smart Grid on the distribution system may impact the reliability of the bulk power system. Pass-through attacks from the distribution system may also present a threat to bulk power system reliability.
Reliability Considerations

- Coordination of controls and protection systems
- Cyber security in planning, design, and operations
- Ability to maintain voltage and frequency control
- Disturbance ride-through (& intelligent reconnection)
- System inertia – maintaining system stability
- Modeling harmonics, frequency response, controls
- Device interconnection standards
- Increased reliance on distribution-level assets to meet bulk system reliability requirements
System Reliability Benefits

- Two-way flow of energy and communications enabling new technologies to supply, deliver and use electricity.

Functions

- Enhanced flexibility and control
- Balancing variable demand & resources (storage, PHEV, etc.)
- Demand response integration
- Large deployment of sensor & automation technologies (wide-area situational awareness)
- Congestion management
- Voltage stability (transient & post-transient stability)
- Frequency regulation, oscillation damping
- Disturbance data monitoring/recording
- Integrating increased amounts of distribution-level assets (residential solar panels, PHEV, etc.)
### Input into Certification Process

<table>
<thead>
<tr>
<th>Likelihood – Threats</th>
<th>Likelihood – Vulnerabilities</th>
<th>Impact Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naturally occurring events (regardless of how infrequent)</td>
<td>Communications</td>
<td>Generation sensors</td>
</tr>
<tr>
<td>Untrained and/or distracted personnel</td>
<td>The internet</td>
<td>Generation actuators</td>
</tr>
<tr>
<td>Insiders with malicious intent</td>
<td>Grid complexity</td>
<td>Transmission sensors</td>
</tr>
<tr>
<td>Cyber attack — lone actors (thrill seekers, script kiddies, etc.)</td>
<td>Grid control system complexity</td>
<td>Transmission actuators</td>
</tr>
<tr>
<td>Cyber attack — terrorism</td>
<td>New systems</td>
<td>Distribution sensors</td>
</tr>
<tr>
<td>Cyber attack — nation-states</td>
<td>New device</td>
<td>Distribution actuators</td>
</tr>
</tbody>
</table>

Despite the technical advances expected from smart grid, the greatest potential risk factor remains the individual with access to high-level control system privileges.
How to Address Cyber Risks?

• Need a systematic approach to vulnerability management
  • One-off vulnerability mitigation with little context
• Intrusion Tolerant Systems
  • Networks are already a contested territory
• Advanced scenario training platform for operators and responders
• Greater State Awareness
  • Detect system thrifts and changes (Security inclusive situational awareness)
• Remove implicit data and system trust
  • Monitoring philosophy “guilty until proven innocent”
Effects on NERC Standards

- Balancing
  - DSM proliferation, Frequency Bias and Response Improvements

- Critical Infrastructure Protection
  - Identification of Critical Cyber Assets, Device/System Awareness, Recovery Plans

- Communication
  - Data exchange, loss of communication, communication with load

- Emergency Operating Procedures
  - Self-healing applications, PMU data for restoration, Storage for blackstart

- Facility Design, Connections, and Maintenance
  - Dynamic Ratings, Operating Limits, Transfer Capabilities

- Personnel Performance, Training, and Qualification
  - Enhanced real-time data to improve simulator-based training

- Voltage and Reactive Support
  - SVCs and STATCOMs to automatically be inserted to provide VAR support.
2011 Follow-on Action Plan

- Bulk Power System & Distribution System
  - Control System Interfaces
  - System Stability
  - Modeling Requirements
  - Critical Infrastructure Protection Requirements

- Standard Development Organizations -
  - Continue to provide input on standards development

- Develop Risk Metrics
Integrating Smart Grid Technologies: Bulk Power System

**Devices**
- Disturbance Monitoring Equipment
- Phasor Measurement Units
- Intelligent Electronic Devices
- Transmission Line Sensors
- Storage

**Systems**
- Transmission Dynamic Line Rating
- Special Protection Systems/Schemes
- Advanced Relaying Systems
- State Estimators
- Wide Area Management Systems
Integrating Smart Grid Technologies: Distribution System

Devices
- Advanced Metering Infrastructure
- Power Factor Correction Devices
- Integrated Volt/VAr Control
- Storage

Systems
- Demand-Side Management Programs
- Under-Frequency/Voltage Load Shedding
- Electric Transportation Supply/Demand (V2G)
- Industrial Automation Systems
### Abbreviations:

- **AMI** – Advanced Metering Infrastructure
- **CFL** – Compact Fluorescent Light bulb
- **CLiC** – Current Limiting Conductors
- **DG / DER** – Distributed Generation / Distributed Energy Resources
- **DSCADA** – Distribution Supervisory Control and Data Acquisition
- **DSTATCOM** – Distributed Static Synchronous Compensator
- **DSM** – Demand-Side Management
- **DTM** – Distribution Transformer Monitoring
- **FACTS** – Flexible Alternating Current Transmission Systems
- **HAN** – Home Area Networks
- **IED** – Intelligent Electronic Devices
- **IFM** – Intelligent Fault Management
- **HTS** – High-temperature Superconducting cables/devices
- **PHEV** – Plug-In Hybrid Electric Vehicle
- **PLC** - Power line carrier/communication
- **PMU** – Phasor Measurement Units
- **RTU** – Remote Terminal Units
- **SHN** – “Self-Healing” Networks
- **SST** – Solid State Transfer Switches
- **STATCOM** - Static Synchronous Compensator
- **WAM** – Wide-Area Management
Critical Infrastructure Coordinated Strategic Action Plan

Eric Rollison
Engineer – Reliability of Assessments
High-Impact, Low-Frequency (HILF) Risks

- “Black Swan” events
  - Occur very infrequently, or, in some cases, have never occurred
  - Little real-world operational experience with addressing these risks
  - Generally have the potential to impact many assets at once
  - Catastrophic impacts on the bulk power system and society-at-large
Created a common understanding of three HILF risks

- Coordinated Cyber/Physical Attacks
- EMP/GMD
- Pandemics

Lays the groundwork for the development of an action plan

- 19 Proposals for Action suggested by workshop participants
Monitoring Progress – The Big Picture

NERC Board of Trustees

ESCC
WHAT: Provide leadership, oversight and direction on critical infrastructure strategy, advise the NERC Board of Trustees
HOW: Develop strategy, identify priorities and key initiatives, recommend timelines, oversee progress
KEY PRODUCTS: Strategic Roadmap, periodic direction and support to Joint Steering Group, interface with government

Joint Steering Group
NERC and PC/OC/CIPC leadership
WHAT: Provide leadership and direction to address Coordinated Action Plan
HOW: Develop high-level work plan and timelines, identify resources required
KEY PRODUCTS: Coordinated Action Plan, periodic Status Reports to ESCC

Coordination
WHAT: Support Joint Steering Group and ESCC
KEY PRODUCTS: Project management support to Task Forces, Status Reports to ESCC

Task Forces
WHAT: Consider options and develop solutions to address Coordinated Action Plan
HOW: Coordinate necessary resources, commit to tasks
KEY PRODUCTS: Whitepaper reports, guidelines, etc.

Electricity entities, government partners, vendors, suppliers
WHAT: Participate on Task Forces
HOW: Contribute time and expertise
Critical Infrastructure Strategic Coordinated Action Plan

Common to All Scenarios
(led by NERC staff, no TF)
- Crisis response plan
- Government interface
- Communications plan
- Information-sharing
- Pandemic

Scope Approved
Dec 2010

Scope Approved
Sep 2010

NERC Technical Committee Leadership
Planning
Operating
Critical Infrastructure Protection

Resources and Expertise
Electricity entities
Vendors
Suppliers
Government partners

Smart Grid Cyber Security TF
Severe-Impact Resilience TF Scope
Spare Equipment Data TF
Cyber Attack TF
Geomagnetic Disturbance TF

NERC Technical Committee Leadership

Critical Infrastructure Protection

Resources and Expertise
Electricity entities
Vendors
Suppliers
Government partners
Defined Scope for Each Task Force

- **Physical Attack**
  - **Mitigate**
    - Cyber Attack TF (CA TF)
    - Severe Impact Resilience TF (SIR TF)
  - **Recover**
    - Spare Equipment Database TF (SED TF)

- **Cyber Attack**
  - **Prevent**
    - Assess Current Capability
  - **Mitigate**
    - Protect or Isolate
    - Withstand and Restore
  - **Recover**
    - Identify Critical Spares

- **Geomagnetic Disturbance**
  - **Prevent**
    - Assess Current Capability
  - **Mitigate**
    - Protect or Isolate
    - Withstand and Restore
  - **Recover**
    - Identify Critical Spares

- **Crisis Response Plan**
- **Communications Plan**
- **Information-Sharing**
- **Government Interface**
Inter-Task Force Coordination

1 – Provide assessment regarding impact of a cyber attack on essential operator tools and communications.
2 – Identify essential operator tools and communications.
3 – Model the impact of GMD, identify system conditions that operators would face.
4 – Provide assessment regarding value of greater advance warning to operators.
5 – Provide assessments regarding number and type of critical equipment damaged.
6 – Identify critical equipment with limited supply and long delivery times.
ESCC Roadmap & Technical Committee Action Plan

- Joint DOE and NERC: *High Impact, Low Risk Event Risk to the North American Bulk Power System*
  

- ESCC: *Critical Infrastructure Strategic Roadmap*
  
  [http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf](http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf)

- Technical Committees: *Critical Infrastructure Strategic Initiatives Coordinated Action Plan*
  
Chair and Vice Chair have been appointed:

- Chair: Donald Watkins – Bonneville Power Administration
- Vice Chair: Frank Koza – PJM Interconnection


- Manufacturers: ABB, Siemens, GE Prolec, Efacec, Schweitzer Relays
- Governmental: US (DOE, DHS, State, and NOAA) and Canada (NR Can, DPS)
Severe Impact Resilience TF Status

- Chair and Vice Chair
  - Chair: Paul Johnson – American Electric Power
  - Vice Chair: Tom Bowe – PJM Interconnection

- Reports to NERC’s Operating Committee

- The SIRTF will provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from three severe-impact events
  - Coordinated physical attack
  - Coordinated cyber attack
  - Geomagnetic disturbance

- Reports to NERC’s Operating Committee
Smart Grid Cyber Security TF Status

- Chair and Vice Chair
  - Chair: Paul McCurley – NRECA
  - Vice Chair: Currently Unfilled

- Four Follow on Subgroup Tasks
  - 1. Integration of smart grid devices/systems onto the bulk power system requires development of new planning/operating tools, models and analysis techniques
  - 2. Integration of smart grid devices/systems will change the character of the distribution system, potentially affecting bulk power system reliability
  - 3. Engage Standard Development Organizations in the U.S. and Canada to increase Coordination and Harmonization in standard development
  - 4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration
Status – Coordinated Action Plan
NERC Priority Initiatives

Geomagnetic Disturbance
- Define objectives
- Warning limitations, mitigation
- Restoration abilities
- Performance requirements
- Restoration abilities
- GMD workshop
- Prevention approaches

Cyber Attack
- Attack tree analysis
- Operator cyber certification
- Cyber security monitoring
- GridEx Summit
- Operator cyber certification

Severe Impact Resilience
- Warning limitations, mitigation
- Operator cyber certification
- DHS bi-directional info sharing
- Operator cyber certification
- DHS bi-directional info sharing
- NLE New Madrid
- NLE New Madrid

Spare Equipment Database
- Define objectives
- Streamlined processes
- Performance requirements
- Streamlined processes
- NERC crisis/communications plan

Other Initiatives
- Milestone deliverables
- NERC crisis/communications plan
- Policy-level severe impact scenario
- NERC crisis/communications plan

Scope Approved
Resources In-Place
Work Underway
Milestone deliverables
Question & Answer
UNITED STATES OF AMERICA  
FEDERAL ENERGY REGULATORY COMMISSION  

Smart Grid Interoperability Standards  
Docket No. RM11-2-000  

SUPPLEMENTAL NOTICE REQUESTING COMMENTS  

(February 16, 2011)  

1. On January 31, 2011, Federal Energy Regulatory Commission (Commission) staff held a technical conference in this proceeding to obtain further information to aid the Commission’s determination of whether there is “sufficient consensus” that certain smart grid interoperability standards are ready for Commission consideration in a rulemaking proceeding, as directed by section 1305(d) of the Energy Independence and Security Act of 2007 (EISA), which requires that:

At any time after the [National Institute of Standards and Technology’s (NIST)] work has led to sufficient consensus in the Commission’s judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.[1]

In light of the discussion among panelists at the conference, staff seeks specific comment on the questions below. Commenters may also provide their views on any of the topics raised at the conference.

2. On July 16, 2009, the Commission issued a Smart Grid Policy Statement[2] in which, among other things, the Commission explained its view that EISA does not make any smart grid standards mandatory and does not give the Commission authority to make or enforce any such standards. The Commission clarified that, under current law, its authority, if any, to make smart grid standards mandatory must derive from the Federal Power Act (FPA).[3] Similarly, its authority to allow rate recovery of smart grid costs must

---

The Commission concluded that the authority to adopt standards under EISA does not change the scope of the Commission’s ratemaking or reliability jurisdiction. Several panelists at the conference expressed concern that adoption of a smart grid standard by the Commission under EISA could lead either the Commission or other regulators, such as state utility regulators, to effectively enforce compliance with the standard by, for example, requiring compliance in order to receive cost recovery or to avoid penalties for non-compliance. Staff seeks comment on the following questions:

- In your view, would making standards enforceable best serve the intent of Congress to facilitate development and use of interoperability standards? Please explain.
- How does the determination of sufficient consensus implicate the requirement to “institute a rulemaking proceeding to adopt” standards and protocols? Please explain.
- What meaning should the Commission give to the phrase “as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets?” Should the Commission evaluate for adoption only those standards that are critical for applications and that may implicate the functionality and interoperability of interstate transmission or wholesale electricity markets?
- How does the smart grid review process consider and evaluate “normative references” (i.e., standards embedded within candidate standard for adoption, needed in order to comply with the standard)?
- How does the NIST process assure that a standard has undergone sufficient review of interoperability and cyber security and is ready for consideration by regulators?

3. Staff seeks comment on ways in which “sufficient consensus” may be defined and used by the Commission to fulfill the purposes of EISA with respect to the appropriate venue for determining and documenting consensus, whether individual attributes of standards require documentation of consensus, and the appropriate role of testing and certification:

- Should the Commission rely solely on the results of the NIST process, and not conduct independent analysis with respect to consensus? If the Commission were to define consensus in this manner, what changes, if any, would be required to the currently effective NIST process?
- Alternatively, should the Commission independently determine consensus? If so, how?
What benefit does documentation of key attributes of a standard (cyber security, functionality, architectural relevance, interoperability, reliability, and implementation issues) bring? Is it necessary? Are there other attributes that should be included, or are any of the attributes noted here unnecessary?

Is it appropriate for reliability and implementation issues to be reviewed by a separate panel, as some panelists commented at the technical conference, composed of utility representatives and NERC?

How should testing and certification for cyber security requirements be incorporated into the adoption process?

Several commenters made the point that the process used for the five families of standards differs from the going forward process. Given that the first five families of standards have been posted for consideration, and a number of commenters at the technical conference point to deficiencies in the process used to identify those standards as ready for consideration, staff requests comment on:

Whether there is a need for additional process concerning the five families of standards and if so, how, for example, the identified cyber security issues can be addressed given the NIST and FERC structures and the language of EISA.

Whether the criteria for the Commission’s evaluation should differ for interoperability and functionality, and the extent to which cyber security is an element of each.

What are the key smart grid benefits that standards should enable? How can the Commission encourage the standards development process to incorporate the continual, but gradual, growth in functionality that is occurring in smart grid implementations and pilot programs?

Persons wishing to comment on the issues discussed above, or any other topic raised at the technical conference, should submit comments to the Commission no later than March 9, 2011. Reply comments should be submitted by March 23, 2011.

Kimberly D. Bose,
Secretary.
UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

SMART GRID INTEROPERABILITY STANDARDS

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON THE JANUARY 31, 2011 TECHNICAL CONFERENCE

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

April 8, 2011
# TABLE OF CONTENTS

I. INTRODUCTION .................................................. 1

II. NOTICES AND COMMUNICATIONS .......................... 2

III. BACKGROUND .................................................. 2

IV. RESPONSES TO QUESTIONS RAISED IN THE FEBRUARY SUPPLEMENTAL NOTICE ...................... 4

V. CONCLUSION ..................................................... 9
I.  INTRODUCTION


Because NERC’s mission, as the FERC-designated Electric Reliability Organization (“ERO”),\(^3\) is to ensure the reliability of the bulk power system in North America by, in part, developing and enforcing mandatory Reliability Standards, NERC’s comments herein focus primarily on three questions related to the impact of the smart grid interoperability standards on reliability.


\(^{2}\) Supplemental Notice Requesting Comments, Docket No. RM11-2-000 (February 16, 2011).

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Holly A. Hawkins*
Assistant General Counsel
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Willie L. Phillips*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

*Persons to be included on the Commission’s service list are indicated with an asterisk. NERC requests waiver of the Commission’s rules and regulations to permit the inclusion of more than two people on the service list.

III. BACKGROUND

On October 6, 2010, the United States National Institute of Standards and Technology (“NIST”) identified in a letter to the Commission five foundational families of smart grid standards for consideration.4 In its letter, NIST stated that it “developed a collaborative process that engages Smart Grid stakeholders in identifying prospective interoperability standards and evaluating these specifications against selected criteria, which include considerations such as stakeholder consensus, domains of applicability, and especially cyber security.”5

---

5 Id.
On January 31, 2011, FERC held a technical conference to discuss whether there was “sufficient consensus”\(^6\) that the proposed NIST smart grid interoperability standards were ready for Commission consideration in a rulemaking proceeding, as directed by section 1305(d) of the Energy Independence and Security Act of 2007 (“EISA”). Section 1305(d) of the EISA provides that:

> At any time after the Institute’s work has led to sufficient consensus in the Commission’s judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.

NIST has formed the Smart Grid Interoperability Panel ("SGIP") to provide an open process for stakeholders to participate in the development of smart grid standards. Although the SGIP does not write standards, it serves as a forum to identify applicable standards, gaps in currently available standards, and priorities for new standardization activities for the evolving smart grid.

As an initial matter, NERC notes that the framework for reviewing smart grid standards used by the SGIP could be improved to achieve greater transparency. At a high level, NERC understands that the first step in the current SGIP process is to identify experts to develop requirement objectives through a Priority Action Plan ("PAP").\(^7\) Then Standards Development Organizations ("SDOs") are selected to create the standard or fill the gap in an existing standard. When the objectives developed by the PAP are completed by the SDOs, the PAP can make a formal request to the SGIP Architecture Committee ("SGAC")\(^8\) and the Cyber Security Working

---

\(^6\) See February Supplemental Notice at P 1.


Group (“CSWG”)⁹ to review the standards against their interoperability, architecture, and cyber security requirements. However, in its current form, the SGIP sector representatives do not coordinate their responses with sectors they represent. This flaw may result in standards not meeting industry needs.

Both the SGAC and CSWG groups can make recommendations regarding proposed standards. Once the SGAC and CSWG reviews are complete, the PAP can develop a package of standards to be included in the Catalog of Standards (“CoS”) and presented to the SGIP Governing Board. The package includes recommendations from individual groups (e.g., CSWG and SGAC) which are prepared through a consensus process. The groups are made up of various stakeholder categories (e.g., vendors, utilities, consultants, academia, and government).¹⁰

NERC supports efforts by NIST to revise the SGIP process, in coordination with industry stakeholders, so that the framework for reviewing smart grid interoperability standards is clear and transparent to all participants. As part of this enhancement, NERC recommends that SGIP representatives coordinate their responses with the stakeholders they represent.

IV. RESPONSES TO QUESTIONS RAISED IN THE FEBRUARY SUPPLEMENTAL NOTICE

In the February Supplemental Notice, FERC acknowledged that Section 1305(d) of the EISA did not make any smart grid standards mandatory and does not give the Commission authority to make or enforce such standards.¹¹ Moreover, the Commission noted that under current law, its authority to approve smart grid interoperability standards as mandatory must

---


¹¹ February Supplemental Notice at P 2 (citing Smart Grid Policy, 128 FERC ¶ 61,060 (2009)).
derive from the Federal Power Act (“FPA”). Accordingly, FERC sought comment on questions pertaining to the FERC’s authority under the FPA and Section 1305(d).

In formulating its response to the February Supplemental Notice, NERC posted to its website Directional Topics to FERC’s Request for Comment on Smart Grid Interoperability Standards, seeking input from industry stakeholders, including the Planning, Operating and Critical Infrastructure Protection committee members regarding the content of NERC’s response. In that posting, NERC provided reliability considerations and sought input on the three questions discussed below.

- How does the NIST process assure that a standard has undergone sufficient review of interoperability and cyber security and is ready for consideration by regulators?

NERC Response

The development of the smart grid interoperability standards currently coordinated by NIST is directed to enhance communications between devices and equipment rather than the operation of the bulk power system of North America. NERC’s Reliability Standards are designed to ensure the reliability of the bulk power system and apply to facilities of the bulk power system. Devices from an array of manufacturers are coordinated to perform multiple control and monitoring functions on generation and transmission to operate the bulk power system of North America. This includes the development of NERC Reliability Standards designed to ensure the protection of cyber assets that are part of the bulk power system.12 To the extent that the NIST interoperability standards will require designers, vendors, and related

---

entities to adopt requirements to lessen the risk of cyber penetration, the proposed interoperability standards should be vetted by industry prior to implementation.\textsuperscript{13}

The most effective approach to ensure industry support for the final smart grid interoperability standards is to ensure thorough assessments of deployments. This includes experience gained from industry demonstration and testing, including design specification, field deployment, model development and overall assessment of performance.

- **Is it appropriate for reliability and implementation issues to be reviewed by a separate panel, as some panelists commented at the technical conference, composed of utility representatives and NERC?**

**NERC Response**

NERC is supportive of reviewing reliability and implementation issues by a separate panel composed of utility representatives and NERC, especially for those issues addressing the management of risk to the reliability, security, and resilience of the bulk power system. As part of the successful integration of smart grid devices and systems, the panel could focus on testing and validation approaches vital to ensure expected benefits are realized, without increased risk to reliability.

- **Whether the criteria for the Commission’s evaluation should differ for interoperability and functionality, and the extent to which cyber security is an element of each.**

**NERC Response**

As noted above, NERC’s primary mission is to ensure the reliability of the bulk power system of North America, and NERC understands the large and increasing role that cyber security occupies in achieving that goal. NERC believes that FERC’s evaluation should take

\textsuperscript{13} NERC Reliability Standards are developed through an American National Standards Institute accredited process: http://www.nerc.com/docs/standards/sar/Appendix_3A_Standard_Processes_Manual_20100903_2_.pdf.
into account whether the cyber security component impacts the reliable operation of the bulk power system.

A secure critical infrastructure is vitally dependent upon cyber security being engineered in emerging technologies. The legacy paradigm of retrofitting solutions for cyber security should be transformed. Cyber security must be considered at the earliest phases of the smart grid standard development, rather than as an add-on to existing communication protocols.

Cyber security issues are germane both to device functionality and interoperability; however, it is reasonable to expect differing evaluation criteria for each category. Confidentiality, integrity, and availability must be addressed, both for data at rest and data in transit. Remote controls (e.g., automated disconnect) must be tightly secured. Moreover, particular attention must be paid to privacy issues, where disclosure of even the most obfuscated usage patterns could facilitate physical attack. In addition, endpoint controls must be robust to maintain the reliability of the bulk power system.

Cyber security is an element in both interoperability and functionality. For example, data protection through encryption should be specified as an essential function, due to the sensitive and personal nature of individual usage patterns that can be tied to a specific person or household. In order for encryption to work across multiple vendor products and implementations, it must be specified to operate seamlessly between those different implementations, thus, it should be specified for interoperability. Similarly, event records for troubleshooting both operational and security issues should be specified functionally, and should be specified to follow a common format across vendor implementations.

Interoperability for cyber security will be essential for different solutions to be able to interact; therefore, the criteria for approving interoperability standards will be important to the
overall smart grid effort. Cyber security controls that do not seamlessly interoperate will result in wasted resources and will cause confusion by having different incompatible solutions that attempt to solve the same problem. Evaluation for interoperability should focus on the ability of different solutions to operate and communicate with each other in a cyber secure fashion, even if the end result is not the most optimal or efficient solution.

Functionality, on the other hand, does not require the same level of evaluation. Different functional solutions should be accepted, because each functional solution is potentially attempting to resolve a slightly different problem in a different way. Evaluation for functionality should focus on providing solutions that meet real needs, and should focus on whether the proposed solution efficiently and effectively resolves the problem being posed.

The strength of the interoperability design of smart grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability through a variety of entrance and exit points. Many of the systems implemented using existing smart grid technologies are designed for control functionality and are not responsive to errors resulting from misuse, miscommunications, or information technology system failures. Security of these control systems can be intentionally defeated or unintentionally corrupted by the installation of software updates, for example.

Improvements will be required to provide robust protection from information technology and communication system vulnerabilities. “Defense-in-Depth” approaches, when coupled with risk assessment, can provide an overarching organizational approach to cyber security management. Use of risk assessment can also help determine appropriate defensive measures.
V. CONCLUSION

NERC respectfully requests that the Commission: 1) support NIST efforts to increase the transparency and representation activities of the SGIP process; 2) support industry testing, demonstration, and validation of the NIST smart grid interoperability standards; 3) create a separate panel composed of utility representatives and NERC to address the management of risk to the reliability, security, and resilience of the bulk power system; and 4) investigate the use of “defense-in-depth” and risk assessment to address cyber security implications of smart grid applications, consistent with these comments.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

/s/ Willie L. Phillips
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net
CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 8th day of April, 2011.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric
Reliability Corporation
Purpose and Deliverables

The purpose of the Task Force is to assess the reliability impacts of integrating Smart Grid technology on the bulk power system. The Task Force has prepared a report, titled *Reliability Considerations from the Integration of Smart Grid* which reviewed Smart Grid characteristics, identifies reliability concerns including cyber-security vulnerability, and provides recommendations to NERC and the industry. The task force will now complete the work plan outlined in this report, including:

1. Integration of smart grid devices/systems requires development of new planning/operating tools, models and analysis techniques
2. Integration of smart grid devices/systems will change the character of the distribution system, potentially affecting bulk power system reliability
3. Engage Standard Development Organizations in the U.S. and Canada to increase coordination and harmonization in standard development
4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

Approach and Milestones

Follow-on work for these tasks will focus on those smart grid devices/systems that are most likely to have an impact on planning and operations. These efforts address Item #K (Smart Grid Security) of the ESCC Critical Infrastructure Strategic Roadmap and the Technical Committee Critical Infrastructure Protection Coordinated Action Plan.2

---


---
1. **Integration of smart grid devices/systems onto the bulk power system requires development of new planning/operating tools, models and analysis techniques**

   The goal of this effort is to identify the tools and models needed by planners and operators to ensure the reliability of the bulk power system is maintained with the integration of smart grid devices/systems.

   **SGTF - Planning/Operations Subgroup**
   - **Start Date:** 1st Qtr. 2011
   - **End Date:** 2nd Qtr 2012

   Review modeling requirements for planning/operations to measure and understand system performance while accommodating smart grid integration:

   - Identify bulk power system modeling requirements for bulk power level smart grid devices/systems, communications, IT and control system interfaces.
   - Evaluate how to include cyber security and control system interfaces into planning/operations simulations to enhance control system security.
   - Assess the impact of bulk system smart grid devices/systems on system stability.
   - Review the Modeling, Data and Analysis (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements.
   - Provide input into smart grid security and NERC’s Standards processes as applicable.

2. **Integration of smart grid devices/systems will change the character of the distribution system, potentially affecting bulk power system reliability**

   The primary goal of this group is to assess if the changes promulgated by the smart grid devices/systems on the distribution system can affect bulk power system reliability.

   **SGTF - Planning/Operations Subgroup**
   - **Start Date:** 1st Qtr. 2011
   - **End Date:** 4th Qtr 2012

   Review existing and new distribution smart grid devices/systems and assess if there are any potential failure modes that might be introduced by their integration.

   - Identify bulk power system modeling requirements for distribution level smart grid devices/systems, communications, IT and control system interfaces.
   - Evaluate how to include the affects of distribution-level cyber security and control system interfaces in the modeling/simulation of bulk power systems.
   - Assess the impact of distribution smart grid system devices/systems on system stability.
   - Review the Modeling, Data and Analysis Standards (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements.
   - Provide input into smart grid security and NERC’s Standards processes as applicable.
3. Engage Standard Development Organizations in the U.S. and Canada to increase Coordination and Harmonization in standard development

The primary goal of this effort is to form liaisons with U.S., Canadian standard setting groups to ensure they are coordinated and harmonized to support reliability.

SGTF - Cyber Security  
Start Date: 1st Qtr. 2011  
End Date: 4th Qtr 2013

Create pathways for harmonization and coordination.

- Monitor smart grid developments and remain engaged in its evolution (Federal/State/Provincial efforts, ISO/RTO, IEEE/IEC, etc.)
- Review existing and new standard developments
- Identify those standards that are vital to bulk power system reliability, including cyber and control system security
- Work with Canadian and US standards setting organizations to ensure coordination and harmonization of vital standards
- Report back on ongoing activities to the PC and CIPC

4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

The primary goal of this effort is to further refine “Defense-in-Depth” and risk assessment approaches to manage cyber and physical security with smart grid integration

SGTF - Cyber Security  
Start Date: 1st Qtr. 2011  
End Date: 4th Qtr 2012

Refine and test “Defense-in-Depth” and risk assessment approaches

- Further refine technical methods
- Identify characteristics that should be measured to provide a current reference and future system measurement
- Form metrics of performance and risk
- Pilot the approach for bulk power system application
- Further refine as required
- Develop a report outlining the methods and documenting the results
- Report back on ongoing activities to the PC, OC and CIPC

Background

The integration of Smart Grid and associated technologies into many levels of the electric system may have bulk power system reliability considerations. While wise Smart Grid integration may present significant opportunities to improve monitoring, security, and power flow, a failure to adequately address the reliability considerations in the planning, design, and operation of the bulk power system could present reliability risks and challenges. While many of the technologies currently associated with Smart Grid have
been available for several years, others are yet unproven; and a rapid integration of all these devices with their associated control and data systems will present significant change in the electric industry that may potentially impact bulk power system reliability. Further, as interoperability has been proposed as the foundation for Smart Grid functions, cyber-security reliability considerations should be integrated to ensure bulk power system reliability is maintained.

Therefore, this NERC task force will review the implications of Smart Grid integration on power system planning, design, security, and operations as well as review NERC’s Reliability Standards to identify any enhancements and gaps.

Membership

NERC will seek task force membership from industry, security, and vendor subject matter experts, with final selection subject to the approval of the chair of the Planning Committee. Members must be willing to commit their time to participate in the task force discussions and contribute to writing the final report.

Each member may designate one alternate to ensure availability. Leadership positions (Chair and, if required, Vice Chair) will be approved by the chair of the Planning Committee.

Initially, the Task Force will be organized as outlined below:

- **Leadership Team**
  - Chair
  - Vice Chair (if required)
  - Team leaders
    - Planning/Operations Tools, models and analysis techniques
    - Distribution System Implications
    - Standard Development Organization Harmonization
    - Physical/Cyber risk metrics for use in smart grid deployment
- **Liaisons from**
  - Demand Response Data Task Force (DRDTF), Critical Infrastructure Protection Committee, Operating Committee, National Institute of Science and Technology (NIST), and the National Energy Board - Canada
- **Members**
- **Observers**
- **NERC Staff**
**Governance**

The task force reports to the Planning Committee and its final work products will be subject to PC review and approval.

**Meeting**

Meeting and conference calls will be scheduled as needed.

*Approved by the Planning Committee: December 8, 2010*
Follow-on work for this task force will focus on those smart grid devices/systems that are most likely to have a material impact on planning and operations. While there may be some interest in investigating the broad range of various issues and technologies related to smart grid, a focused approach on specific technologies will have significant value for reliability of the bulk power system and future NERC programs and activities. These efforts address Item #K (Smart Grid Security) of the ESCC Critical Infrastructure Strategic Roadmap and the Technical Committee Critical Infrastructure Protection Coordinated Action Plan.1

1. **Integration of smart grid devices and systems onto the bulk power system requires development of new planning and operating tools, models, and analysis techniques**

   Identify the tools and models needed by planners/operators for successful integration of smart grid devices and systems

   **SGTF – Planning/Operations Subgroup**  
   **Start Date:** 1st Qtr. 2011  
   **End Date:** 2nd Qtr 2012

   Review modeling requirements for planning and operations to measure and understand system performance while accommodating smart grid integration as follows:
   - identify bulk power system modeling requirements for bulk power level smart grid devices/systems, communications, IT, and control system interfaces;
   - evaluate how to include cyber security and control system interfaces into planning/operation simulations to enhance control system security;
   - assess the affect of bulk system smart grid devices/systems on system stability;
   - Determine successful integration considerations to ensure reliability
   - review the Modeling, Data, and Analysis (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and
   - provide input into smart grid security and NERC’s Standards processes as applicable.

2. **Integration of smart grid devices/systems will change the character of the distribution system**

   Assess reliability considerations that need to be addressed with the integration of large amounts of smart grid devices and systems on the distribution system

   **SGTF – Planning/Operations Subgroup**  
   **Start Date:** 1st Qtr. 2011  
   **End Date:** 4th Qtr 2012

   Review existing and new distribution smart grid devices and systems and assess if there are any potential failure modes that they need to address as part of their integration as follows:
   - identify bulk power system modeling requirements for distribution-level smart grid devices/systems, communications, IT, and control system interfaces;

---

1 See agenda item 2 of [http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf](http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf) and [http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf](http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf)
• evaluate how to include the affects of distribution-level cyber security and control system interfaces in the modeling/simulation of bulk power systems;

• assess the impact of distribution smart grid system devices/systems on system stability;

• Determine successful integration considerations to ensure reliability

• review the Modeling, Data and Analysis Standards (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and

• provide input into smart grid security and NERC’s Standards processes as applicable.

3. **Engage Standard Development Organizations in the U.S. and Canada to increase coordination and harmonization in standard development**

   Form liaisons with U.S. and Canadian standards-setting groups to ensure coordinated and harmonized standards to support reliability

   **SGTF – Cyber Security**  **Start Date: 1st Qtr. 2011**  **End Date: 4th Qtr 2013**

   Create pathways for harmonization and coordination as follows:

   • monitor smart grid developments and remain engaged in its evolution (federal/state/provincial efforts, ISO/RTO, IEEE/IEC, etc.);

   • review existing and new standards developments;

   • indentify those standards that are vital to bulk power system reliability, including cyber and control system security;

   • work with Canadian and U.S. standards-setting organizations to ensure coordination and harmonization of vital standards; and

   • report back on ongoing activities to the PC and CIPC.

4. **Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration**

   Further refine defense-in-depth and risk assessment approaches to manage cyber and physical security with smart grid integration.

   **SGTF – Cyber Security**  **Start Date: 1st Qtr. 2011**  **End Date: 4th Qtr. 2012**

   Refine and test defense-in-depth and risk assessment approaches as follows:

   • further refine technical methods;

   • identify characteristics that should be measured to provide a current reference and future system measurement;

   • form metrics of performance and risk;

   • pilot the approach for bulk power system application;

   • further refine as required;

   • develop a report outlining the methods and documenting the results; and

   • report back on ongoing activities to the PC, OC, and CIPC.
Appendix 2: Follow-on Work Plan

Follow-on work for this task force will focus on those smart grid devices/systems that are most likely to have a material impact on planning and operations. While there may be some interest in investigating the broad range of various issues and technologies related to smart grid, a focused approach on specific technologies will have significant value for reliability of the bulk power system and future NERC programs and activities. These efforts address Item #K (Smart Grid Security) of the ESCC Critical Infrastructure Strategic Roadmap and the Technical Committee Critical Infrastructure Protection Coordinated Action Plan.\(^1\)

1. Integration of smart grid devices and systems onto the bulk power system requires development of new planning and operating tools, models, and analysis techniques. Assess reliability considerations that need to be addressed with the integration of large amounts of smart grid devices and systems on the distribution system.

2. Identify the tools and models needed by planners/operators for successful integration of smart grid devices/systems. Assess reliability considerations that need to be addressed with the integration of large amounts of smart grid devices and systems on the distribution system.

   ▶ Autonomously operated grid self healing systems could significantly affect under voltage, under frequency and manual load shed systems – these systems should be able to interact, communicate and take coordinated actions and accurately defining the problem statement:
   
   ▶ Experiences and lessons learned from initial smart grid deployments

   ▶ Identify bulk power system modeling requirements for bulk power level smart grid devices/systems, communications, IT, and control system interfaces:
   
   ▶ Such as load demand modeling, ...?

   ▶ DER programs are only focusing only on load not committed to DER programs, not overall impacts on the grid

   ▶ DG as a subset of this problem

   ▶ Reference IVGTF reports on Wind Generation and bring as much of that work into this paper

   ▶ Example – Large amounts of wind coming online in MISO interfering with interfaces in PJM during light load periods and forcing other traditional generation sources offline – storage at wind farms

   ▶ Demand Dispatch for frequency issues

   ▶ Operational study on distributed generation and storage can alleviate transmission congestion on the system

---

\(^1\) See agenda item 2 of [http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf](http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf) and [http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf](http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf)
Appendix 2: Follow-on Work Plan

- Customer Price response programs in a smart grid – Need comprehensive list of definitions to eliminate confusion across different programs – reaction between price signal and reliability needs
- Microgrid development and its potential impact development and transmission reliability
  - Reference publications on distributed generation that exist in Denmark and Germany
  - Hawaii has similar issues as well
  - Uncertainty around load models and how the system will have to dynamically react in the future rather than having pre-planned actions months in advance
  - Potentially revisit devices and systems and determine what impact they would have on bulk power system modeling
- Evaluate how to include cyber security and control system interfaces into planning/operation simulations to enhance control system security;
- What additional types of Real-time Data are being generated by Smart Grid Devices and have to be considered to maintain Reliability
  - Such as the performance and capacity of back-end IT systems to handle
  - Generating a historical database to operate and plan the system for the future
  - Changing load shape and determining how that impacts reliability as more demand may be served by base load
  - How distributed generation impacts inertia and how to analyze and quantify the impacts associated with offsetting one resource from other – the trend towards smaller plants and renewable resources
- The risks of combining all of the information into a central data store which will need to have risk management software to mitigate critical infrastructure vulnerabilities
- Differences in power quality between distributed sources and traditional sources
  - assess the affect of bulk system smart grid devices/systems on system stability;
  - Determine successful integration considerations to ensure reliability
  - Expanding contingency planning reach out into the communications infrastructure and its impact on reliability – and the duration of these impacts. Are these impacts for minutes, hours, or days?
    - Renewables may encourage further analysis and evaluation of transmission options (AC versus DC) for the resources to be brought to the bulk power system and enhance reliability of the grid
    - Impact of regulations on quick reacting resources that are beyond the purview of electricity regulators (such as EPA regulations)
- review the Modeling, Data, and Analysis (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and
- provide input into smart grid security and NERC’s Standards processes as applicable.
Appendix 2: Follow-on Work Plan

3. SGTF – Planning/Operations Subgroup  Start Date: 1st Qtr. 2011  End Date: 4th Qtr 2012
Review existing and new distribution smart grid devices and systems and assess if there are any potential failure modes that they need to address as part of their integration as follows:

- Identify bulk power system modeling requirements for distribution-level smart grid devices/systems, communications, IT, and control system interfaces;
- Evaluate how to include the affects of distribution-level cyber security and control system interfaces in the modeling/simulation of bulk power systems;
- Assess the impact of distribution smart grid system devices/systems on system stability;
- Determine successful integration considerations to ensure reliability;
- Review the Modeling, Data and Analysis Standards (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements; and
- Provide input into smart grid security and NERC’s Standards processes as applicable.

4. Engage Standard Development Organizations in the U.S. and Canada to increase coordination and harmonization in standard development
Form liaisons with U.S. and Canadian standards-setting groups to ensure coordinated and harmonized standards to support reliability

SGTF – Cyber Security  Start Date: 1st Qtr. 2011  End Date: 4th Qtr 2013
Create pathways for harmonization and coordination as follows:

- Draft a list of standards that currently affect the bulk power systems
- Then determine if they are devices or technology versus users or the what and how that we had discussed earlier
- Common practices and regulations that current
- List SDO that go with the standards and regulations
- List where these standards and regulations and are applicable
- Listing organizations that are evaluating standards and
- Identification of any gaps in how they evaluating them
- How can NERC, the industry, and regulators fill in the gaps
- Setup a guide or data base to track all of these ongoing activities
- Operational, Planning, etc… (can be more – just examples) practices that become unofficial standards

- Monitor smart grid developments and remain engaged in its evolution (federal/state/provincial efforts, ISO/RTO, IEEE/IEC, etc.);
- Review existing and new standards developments;
- Identify those standards that are vital to bulk power system reliability, including cyber and control system security;
work with Canadian and U.S. standards-setting organizations to ensure coordination and harmonization of vital standards; and

report back on ongoing activities to the PC and CIPC.

5. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

Further refine defense-in-depth and risk assessment approaches to manage cyber and physical security with smart grid integration.

SGTF – Cyber Security  Start Date: 1st Qtr. 2011  End Date: 4th Qtr. 2012

Refine defense-in-depth and risk assessment approaches as follows:

- What risk management frameworks are out there and what are the frameworks are out there to development
- What type of cyber and physical characteristics and metrics should bulk system be keeping track of – characteristics not specifics (voltage, power quality, number of probes, number of devices)
  - Blended attacks which take multiple vectors such as cyber and physical
- Risk of inaccurate data, risk data aggregation, load aggregation, power aggregation, and data storage and communication
- Determining what data is relevant and what is just noise
- Cost of mitigating risk and value of mitigating risk – bang for buck – cost factors and practices rather than defined monetary values
  - This report could recommend using modeling and simulation practices to develop risk metrics – look to models ISA-84
- Framework for metrics that define resilient systems
- Risk of third party devices – supply chain
- Risks of CEII (critical energy infrastructure information) issues
- Which services and features that these devices offer should be standardized and others that should be withdrawn.
- Zone of trust versus zone of vulnerabilities – Review FERC Order 706 directive

Recommendation maybe be to develop testing scenarios – engage National Labs (INL), Universities, and Academic Researchers – be non-specific on risk evaluation – how to review and solve the problem – (DOE) roadmap for secure control systems in the energy sector

- further refine technical methods;
- identify characteristics that should be measured to provide a current reference and future system measurement;
- form metrics of performance and risk;
- pilot the approach for bulk power system application;
- further refine as required;
• develop a report outlining the methods and documenting the results; and
• report back on ongoing activities to the PC, OC, and CIPC.
# Smart Grid Task Force

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Organization</th>
<th>Address</th>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Paul McCurley</td>
<td>National Rural Electric Cooperative</td>
<td>Manager, Power Supply and Chief Engineer</td>
<td>(703) 907-5867</td>
<td></td>
<td><a href="mailto:paul.mccurley@nreca.coop">paul.mccurley@nreca.coop</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(703) 907-5517 Fx</td>
<td></td>
</tr>
<tr>
<td>Vice-Chair Cyber</td>
<td>Sandy Bacik</td>
<td>EnerNex Corp</td>
<td>Principal Consultant</td>
<td>(865) 696-4470</td>
<td></td>
<td><a href="mailto:sandy.bacik@enernex.com">sandy.bacik@enernex.com</a></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chair Research</td>
<td>Marija Ilic</td>
<td>Carnegie Mellon University</td>
<td>Professor</td>
<td>(412) 260-2471</td>
<td></td>
<td><a href="mailto:milic@ece.cmu.edu">milic@ece.cmu.edu</a></td>
</tr>
<tr>
<td>and Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chair Cyber</td>
<td>Christopher Kotting</td>
<td>ThinkSmartGrid</td>
<td>Co-Founder &amp; Regulatory Lead</td>
<td>(614) 657-6483</td>
<td></td>
<td><a href="mailto:ckotting@thinksmartgrid.com">ckotting@thinksmartgrid.com</a></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chair Planning</td>
<td>Paul Myrda</td>
<td>EPRI</td>
<td>Technical Executive</td>
<td>(708) 479-5543</td>
<td></td>
<td><a href="mailto:pmyrda@epri.com">pmyrda@epri.com</a></td>
</tr>
<tr>
<td>and Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chair Planning</td>
<td>Trevor Siegfried</td>
<td>PPL Electric Utilities Corp.</td>
<td>Senior Engineer</td>
<td>(610) 774-5718</td>
<td></td>
<td><a href="mailto:tssiegfried@pplweb.com">tssiegfried@pplweb.com</a></td>
</tr>
<tr>
<td>and Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chair</td>
<td>Virginia Whitaker</td>
<td>United Illuminating Co.</td>
<td>Manager - SCADA</td>
<td>(203) 926-4468</td>
<td></td>
<td><a href="mailto:ginger.whitaker@uinet.com">ginger.whitaker@uinet.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(502) 217-2193 Fx</td>
<td></td>
</tr>
<tr>
<td>Secretary</td>
<td>Eric Rollison</td>
<td>North American Electric Reliability Corporation</td>
<td>Engineer of Reliability Assessments</td>
<td>(404) 446-2560</td>
<td></td>
<td><a href="mailto:eric.rollison@nerc.net">eric.rollison@nerc.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(609) 452-9550 Fx</td>
<td></td>
</tr>
<tr>
<td>Nicholas Abi-Samra</td>
<td></td>
<td>Accenture</td>
<td>Consultant</td>
<td>(760) 576-9464</td>
<td></td>
<td><a href="mailto:nicholas.abi-samra@accenture.com">nicholas.abi-samra@accenture.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(760) 258-9831 Fx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sandy Aivaliotis</td>
<td></td>
<td>Nexans</td>
<td>Senior VP, Operations, Technology, and Business Development</td>
<td>(416) 648-4382</td>
<td></td>
<td><a href="mailto:sandy.aivaliotis@nexans.com">sandy.aivaliotis@nexans.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(203) 431-0296 Fx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharla Artz</td>
<td></td>
<td>Schweitzer Engineering Laboratories, Inc.</td>
<td></td>
<td>(703) 647-6253</td>
<td></td>
<td><a href="mailto:sharla_artz@selgs.com">sharla_artz@selgs.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(703) 647-6259 Fx</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

June 13, 2011
<table>
<thead>
<tr>
<th>Name</th>
<th>Title/Position</th>
<th>Company</th>
<th>Address or Details</th>
<th>Phone Numbers</th>
<th>Email Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sami Ayyorgan, PhD</td>
<td>Director and Senior Scientist</td>
<td>Telcordia Technologies</td>
<td>1 Telcordia Drive, Piscataway, New Jersey 08854-4151</td>
<td>(732) 699-2270</td>
<td><a href="mailto:sami@research.telcordia.com">sami@research.telcordia.com</a></td>
</tr>
<tr>
<td>Scott Baker</td>
<td>Business Solutions Analyst</td>
<td>PJM Interconnection, L.L.C.</td>
<td>955 Jefferson Avenue, Valley Forge CC, Norristown, PA</td>
<td>(610) 666-2235</td>
<td><a href="mailto:bakers1@pjm.com">bakers1@pjm.com</a></td>
</tr>
<tr>
<td>Jonathan Booe</td>
<td>Staff Attorney</td>
<td>North American Energy Standards Board</td>
<td>1301 Fannin, Suite 2350, Houston, TX 77002</td>
<td>(713) 356-0060</td>
<td><a href="mailto:jbooe@naesb.org">jbooe@naesb.org</a></td>
</tr>
<tr>
<td>Joseph Bucciero</td>
<td>President and Executive Consultant</td>
<td>Bucciero Consulting, LLC</td>
<td>3011 Samantha Way, Gilbertsville, PA 19525</td>
<td>(267) 981-5445</td>
<td><a href="mailto:joe.bucciero@gmail.com">joe.bucciero@gmail.com</a></td>
</tr>
<tr>
<td>Joseph G. Callis</td>
<td>Senior Business Solutions Engineer</td>
<td>PJM Interconnection, L.L.C.</td>
<td>955 Jefferson Avenue, Valley Forge Corporate Center, Norristown, PA</td>
<td>(610) 666-3147</td>
<td><a href="mailto:callij@pjm.com">callij@pjm.com</a></td>
</tr>
<tr>
<td>James Calore</td>
<td>Manager - Interconnection Planning</td>
<td>Public Service Electric and Gas Co.</td>
<td>80 Park Plaza, T-13, Newark, NJ 07102</td>
<td>(973) 430-6628</td>
<td><a href="mailto:james.calore@psc.com">james.calore@psc.com</a></td>
</tr>
<tr>
<td>Christopher Campione</td>
<td></td>
<td>Planet Technologies</td>
<td>20400 Observation Drive, Suite 201, Germantown, MD 20876</td>
<td>(301) 721-0100</td>
<td><a href="mailto:rocky@go-planet.com">rocky@go-planet.com</a></td>
</tr>
<tr>
<td>Jay Cappy</td>
<td>Managing Principal - Global Services</td>
<td>Verizon Business</td>
<td>101 Bullitt Lane, Suite 107, Louisville, KY 40222</td>
<td>(502) 395-2811</td>
<td><a href="mailto:jay.j.cappy@verizonbusiness.com">jay.j.cappy@verizonbusiness.com</a></td>
</tr>
<tr>
<td>Lawrence D. Carter</td>
<td>Electrical Engineer/Grid Expert</td>
<td>Bonneville Power Administration</td>
<td>DE-3, P.O. Box 3621, Portland, OR 97208</td>
<td>(360) 931-2477</td>
<td><a href="mailto:ldcarter@bpa.gov">ldcarter@bpa.gov</a></td>
</tr>
<tr>
<td>Sunil Cherian</td>
<td>CEO</td>
<td>Spirae, Inc.</td>
<td>255 Linden St. Suite 201, Fort Collins, CO 80524</td>
<td>(970) 484-8259</td>
<td><a href="mailto:sunil@spirae.com">sunil@spirae.com</a></td>
</tr>
<tr>
<td>Jason D. Christopher</td>
<td>Electrical Engineer - Project Lead, Smart Grid Security</td>
<td>Federal Energy Regulatory Commission</td>
<td>888 First Street, NE, Washington, DC 20426</td>
<td>(202) 502-8256</td>
<td><a href="mailto:jason.christopher@ferc.gov">jason.christopher@ferc.gov</a></td>
</tr>
<tr>
<td>John L. Ciufo, P. Eng.</td>
<td>Principal</td>
<td>Ciufo and Cooperberg Consulting Ltd.</td>
<td>4048 Twine Cres., Mississauga, ON L4Z 1E5</td>
<td>(647) 988-5163</td>
<td><a href="mailto:john.ciufo@bell.net">john.ciufo@bell.net</a></td>
</tr>
<tr>
<td>Mike Cooper</td>
<td>US Transmission R&amp;D</td>
<td>National Grid</td>
<td>40 Sylvan Road, Waltham, MA 02451</td>
<td>(781) 907-2495</td>
<td><a href="mailto:michael.cooper@us.ngrid.com">michael.cooper@us.ngrid.com</a></td>
</tr>
</tbody>
</table>
Tom Dagenais
Senior Transmission Planning Engineer
American Transmission Company, LLC
2 Fen Oak Court
Madison, Wisconsin 53718
(608) 877-7161
tdagenais@atcllc.com

Dave D Dalva
Smart Grid Security Lead
Cisco Systems, Inc.
Surrey, British Columbia V3W 7R7
(703) 484-0129
didalva@gmail.com

Ali Daneshpooy
Program Manager, Smart Utility
Powertech Labs, Inc.
12388 8th Avenue
Surrey, British Columbia V3W 7R7
(604) 590-6684
(604) 992-5167
ali.danesh@powertechlabs.com

Richard DeBlasio
National Renewable Energy Laboratory Program Manager
National Renewable Energy Laboratory
1617 Cole Blvd
Goldebn, Colorado 80401
303-275-4333
303-275-3835
dick.deblasio@nrel.gov

Terry Dillon
System Ana/Intgrtr Ld
Arizona Public Service Co.
2124 West Cheryl Drive
Phoenix, Arizona 85021
(602) 371-5072
terry.dillon@aps.com

Thomas Tom Dion
Control Systems Security Program Manager
DHS National Cyber Security Division
(703) 235-5179
Thomas.dion@hs.gov

Alejandro Dominguez-Garcia
Assistant Professor, Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
1406 West Green Street
MC-702, 341 Everitt Laboratory
Urbana, Illinois 61801
(217) 333-3953
aledan@illinois.edu

Gerald John FitzPatrick
Leader, EEEL Smart Grid Project
National Institute of Standards and Technology
100 Bureau Drive, MS-8172
Gaithersburg, Maryland 20899-8172
(301) 975-8922
(301) 926-3972
Gerald.fitzpatrick@nist.gov

Norm Fraser
Chief Operating Officer
Hydro Ottawa Limited
3025 Albion Road, North
Toronto, Ontario M5B 2C7
(613) 738-5478
(613) 738-6426
normfraser@hydroottawa.com

Amitabha Tab Gangopadhyay
Professional Engineer
National Energy Board
444 Seventh Avenue SW
Calgary, Alberta T2P 0X8
(403) 299-3611
(403) 292-5503
tgangopadhyay@neb-one.gc.ca

Joel Garmon
Director of Information Security
Florida Power & Light Co.
9250 W. Flagler Street
Miami, Florida 33174
(305) 552-3097
(305) 552-3259
joel.garmon@fpl.com

Ed Goff
System Architect - IT&T Security
Progress Energy
100 E. Davie Street
Mail Code: TPP11
Raleigh, North Carolina 27601
(919) 812-2202
edwin.goff@pgmail.com

Krish Gomatom
Analyst - Energy Efficiency & Demand Response Analytics
Electric Power Research Institute
942 Corridor Park Boulevard
Knoxville, Tennessee 37932
(865) 218-8070
(865) 218-8085
kgomatom@epri.com
<table>
<thead>
<tr>
<th>Name</th>
<th>Title and Organization</th>
<th>Address/Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alan Thomas LaBarre</td>
<td>Manager Distribution Planning, National Grid</td>
<td>40 Sylvan Road, Waltham, MA 02451</td>
</tr>
<tr>
<td>Mike LaMarre</td>
<td>Division Manager of Infrastructure Management, Austin Energy</td>
<td></td>
</tr>
<tr>
<td>John Lim, CISSP</td>
<td>Department Manager, IT Infrastructure Planning, Consolidated Edison Co. of New York</td>
<td>4 Irving Place, New York, NY 10003</td>
</tr>
<tr>
<td>Claudio Lima</td>
<td>Managing Director, Smart Grid, Sonoma Innovation</td>
<td>171 Branham Lane, San Jose, CA 94112</td>
</tr>
<tr>
<td>Donald A. Lynd</td>
<td>Senior Engineer, HVD Planning, Consumers Energy</td>
<td>1945 W. Parnall Road, Jackson, MI 49201</td>
</tr>
<tr>
<td>Wade Malcolm</td>
<td></td>
<td>560 Mission Street, Suite 1200, SF, CA 94105</td>
</tr>
<tr>
<td>Jack McCall</td>
<td>Director, Business Development, American Superconductor (AMSC)</td>
<td>15775 W Schaefer Center, New Berlin, WI 53151</td>
</tr>
<tr>
<td>Devin McCarthy</td>
<td>Manager, Distribution, Canadian Electricity Association</td>
<td>350 Sparks, Suite 1100, Ottawa, ON K1R 7S8</td>
</tr>
<tr>
<td>Douglas McGinnis</td>
<td>IT Manager of Communications, Exelon Corporation</td>
<td>2301 Market Street, Philadelphia, PA 19103</td>
</tr>
<tr>
<td>Ralph H. McKosky</td>
<td>Project Manager-Technical Innovations, Tennessee Valley Authority</td>
<td>1101 Market Street, Chattanooga, TN 37402</td>
</tr>
<tr>
<td>Rick Meeker</td>
<td>Program Development Manager - Industry Partnerships, Florida State University</td>
<td>2000 Levy Avenue, Tallahassee, FL 32310</td>
</tr>
<tr>
<td>Bill Menge</td>
<td>Director, Smart Grid, Kansas City Power &amp; Light Co.</td>
<td>1200 Main Street, Kansas City, MO 64105</td>
</tr>
</tbody>
</table>

June 13, 2011
<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Mertz</td>
<td>PNM Resources</td>
<td>Alvarado Square, New Mexico</td>
<td>(505) 241-0676</td>
<td><a href="mailto:michael.mertz@pnmresources.com">michael.mertz@pnmresources.com</a></td>
</tr>
<tr>
<td>Nathan Mitchell, P.E.</td>
<td>American Public Power Association</td>
<td>1875 Connecticut Avenue</td>
<td>(202) 467-2925</td>
<td><a href="mailto:nmitchell@appanet.org">nmitchell@appanet.org</a></td>
</tr>
<tr>
<td>Paul Molitor</td>
<td>NEMA</td>
<td>1300 N. 17th Street, Rosslyn</td>
<td>(703) 841-3262</td>
<td><a href="mailto:paul.molitor@nema.org">paul.molitor@nema.org</a></td>
</tr>
<tr>
<td>Austin Montgomery</td>
<td>NRECA Building, Suite 200</td>
<td>Arlington, Virginia</td>
<td>(703) 908-1110</td>
<td><a href="mailto:amontgom@sei.cmu.cc">amontgom@sei.cmu.cc</a></td>
</tr>
<tr>
<td>Robert Moreland</td>
<td>Duke Energy</td>
<td>400 South Tryon Street</td>
<td>(980) 373-6439</td>
<td><a href="mailto:robert.moreland@duke-energy.com">robert.moreland@duke-energy.com</a></td>
</tr>
<tr>
<td>Ian Mundell</td>
<td>PJM Interconnection, L.L.C.</td>
<td>955 Jefferson Avenue</td>
<td>(610) 666-4617</td>
<td><a href="mailto:mundei@pjm.com">mundei@pjm.com</a></td>
</tr>
<tr>
<td>David Nichols</td>
<td>Altairnano, Inc.</td>
<td>204 Edison Way, Reno</td>
<td>(317) 565-6044</td>
<td><a href="mailto:dnichols@altairnano.com">dnichols@altairnano.com</a></td>
</tr>
<tr>
<td>Thomas Overman</td>
<td>Boeing Defense, Space &amp; Security</td>
<td>884 Hermosa Ct.</td>
<td>(408) 524-3721</td>
<td><a href="mailto:thomas.overman@boeing.com">thomas.overman@boeing.com</a></td>
</tr>
<tr>
<td>James Resek</td>
<td>KEMA Consulting</td>
<td>4377 County Line Road</td>
<td>(215) 674-2000</td>
<td><a href="mailto:Jim.resek@kema.com">Jim.resek@kema.com</a></td>
</tr>
<tr>
<td>Cliff Rosborough</td>
<td>Pepco</td>
<td>701 Ninth Street, N.W.</td>
<td></td>
<td><a href="mailto:cegrosborough@pepco.com">cegrosborough@pepco.com</a></td>
</tr>
<tr>
<td>Brett Edward Sargent</td>
<td>LumaSense Technologies</td>
<td>3301 Leonard Ct., Santa Clara</td>
<td>(404) 512-6336</td>
<td><a href="mailto:b.sargent@lumasenseinc.com">b.sargent@lumasenseinc.com</a></td>
</tr>
<tr>
<td>Venkat Shastri</td>
<td>PCN Technology, Inc</td>
<td></td>
<td>(858) 434-0605</td>
<td><a href="mailto:venkat@pcntechnology.com">venkat@pcntechnology.com</a></td>
</tr>
<tr>
<td>Robert Sean Sherman</td>
<td>Cyber Security</td>
<td>1760 Old Meadow Road</td>
<td>(360) 609-9103</td>
<td><a href="mailto:sean.sherman@zoho.com">sean.sherman@zoho.com</a></td>
</tr>
</tbody>
</table>
Pamela C Zdenek
Regulatory and Compliance Advisor
BP US Cogens
700 Louisiana Street
33rd Floor
Houston, Texas 77002
(713) 354-4830
(713) 225-1326 Fx
pamela.zdenek@bp.com

Observer
JK August
VP Operations
CORE
5915 Braun Way
Arvada, Colorado 80004
(303) 425-7408
(303) 425-0861 Fx
jkaugust@msn.com

Observer
Ken Caird
Senior Systems Engineer
GE Energy
4200 Wildwood Parkway
Atlanta, Georgia 30339
(678) 844-6620
ken.caird@ge.com

Observer
Christopher Eisenbrey
Director, Business Information
Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, D.C. 20004-2696
(202) 508-5574
(202) 508-5599 Fx
ceisenbrey@eei.org

Observer
Mark Fabro
President/Chief Security Scientist
Lofty Perch, Inc.
15-505 Hood Road
Markham, Ontario L3R 5V6
(647) 226-4225
(905) 489-2828 Fx
fabro@loftyperch.com

Observer
Dave Hardin
Staff Engineer
Automation Federation
70 Mechanic Street
Foxboro, Massachusetts 02035
(508) 549-3362
david.hardin@ips.invensys.com

Observer
Ernie N Hayden
Professional Services Consultant
Verizon Business
206-458-8761
ernest.hayden@verizonbusiness.com

Observer
Gavan Jude Howe
President/CEO
Howe Brand Communications
47 Front Street East
3rd Floor
Toronto, Ontario M5E 1B3
(416) 363-6591
(416) 363-6796 Fx
gavan@ebranders.com

Observer
Richard Kalisch
Senior Director Technology Initiatives
Midwest ISO, Inc.
P.O. Box 4202
Carmel, Indiana 46082
(317) 249-5265
(317) 249-5084 Fx
rkalisch@midwestiso.org

Observer
Jeffrey Katz
Chief Technology Officer, Energy and Utilities Industry
IBM
1 Financial Plaza
Hartford, Connecticut 06103
(877) 540-6891
jskatz@us.ibm.com

Observer
Madhav D. Manjrekar
Team Leader
Siemens Corporate Research
755 College Road East
Princeton, New Jersey 08540
(609) 734-6566
(609) 734-3644 Fx
madhav.manjrekar@siemens.com

Observer
James D. McCalley
Professor
Iowa State University
2210 Coover Hall
Dept. of Elec. and Comp. Engg.
Ames, Iowa 50011
(515) 294-4844
(515) 294-4263 Fx
jdm@iastate.edu

Observer
Karen Miu

June 13, 2011
<table>
<thead>
<tr>
<th>Observer</th>
<th>Name</th>
<th>Title</th>
<th>Address</th>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observer</td>
<td>Scott R. Mix</td>
<td>CIP Technical Manager</td>
<td>North American Electric Reliability</td>
<td>(609) 452-8060</td>
<td></td>
<td><a href="mailto:scott.mix@nerc.net">scott.mix@nerc.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Corporation</td>
<td>(609) 452-9550</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>116-390 Village Boulevard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Princeton, New Jersey 08540-5721</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>John Moura</td>
<td>Manager of Reliability Assessments</td>
<td>North American Electric Reliability</td>
<td>(404) 446-2560</td>
<td>(609) 452-9550</td>
<td><a href="mailto:john.moura@nerc.net">john.moura@nerc.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Corporation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3353 Peachtree Road, N.E.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Suite 600, North Tower</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Atlanta, Georgia 30326</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Nelson Muller</td>
<td>Executive Vice President</td>
<td>OATI</td>
<td>(763) 201-2000</td>
<td>(763) 553-2813</td>
<td><a href="mailto:nelson.muller@oati.net">nelson.muller@oati.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2300 Berkshire Lane North</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maildrop F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minneapolis, Minnesota 55441</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Daniel E. Pfeiffer</td>
<td>Vice President of Regulatory Affairs</td>
<td>Itron, Inc.</td>
<td>(509) 891-3839</td>
<td></td>
<td><a href="mailto:dan.pfeiffer@itron.com">dan.pfeiffer@itron.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2111 N. Molter Rd</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Liberty Lake, Washington 99019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Bhasker Rao</td>
<td>CEO</td>
<td>Fortech Software Consulting Inc</td>
<td>(480) 730-0691</td>
<td>(480) 718-8216</td>
<td><a href="mailto:corpmail@fortechsw.com">corpmail@fortechsw.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>430 W. Warner Road #113</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tempe, Arizona 85284</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Marie Rinkoski Spangler</td>
<td>EIA-411 Survey Manager</td>
<td>U.S. Department of Energy</td>
<td>(202) 586-2446</td>
<td>(202) 287-1938</td>
<td><a href="mailto:marie.rinkoski-spangler@eia.doe.gov">marie.rinkoski-spangler@eia.doe.gov</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1000 SW Independence Avenue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BE-060</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Washington, D.C. 20585</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Jesus M. Sierra</td>
<td>Group Manager</td>
<td>Federal Energy Regulatory Commission</td>
<td>(202) 502-8479</td>
<td>(202) 219-2836</td>
<td><a href="mailto:nano.sierra@ferc.gov">nano.sierra@ferc.gov</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>888 First Street NE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Washington, D.C. 20426</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>John P. Skliutas</td>
<td>Principal Engineer</td>
<td>GE Energy</td>
<td>(518) 385-0209</td>
<td>(518) 385-9529</td>
<td><a href="mailto:john.skliutas@ge.com">john.skliutas@ge.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>53-300R, 1 River Road</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Schenectady, New York 12345</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>William Souza</td>
<td>Manager, Security Integration</td>
<td>PJM Interconnection, L.L.C.</td>
<td>(610) 666-2237</td>
<td>(610) 728-4855</td>
<td><a href="mailto:beknh03@gmail.com">beknh03@gmail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>955 Jefferson Avenue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Norristown, Pennsylvania 19403</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Ron Stelmak</td>
<td>Vice President Sales and Marketing</td>
<td>The Valley Group (a Nexans Company)</td>
<td>(203) 431-0262</td>
<td>(203) 241-3513</td>
<td><a href="mailto:ron.stelmak@cat-l.com">ron.stelmak@cat-l.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Charlie Vartanian</td>
<td>Director, Grid Integration</td>
<td>A123 Systems</td>
<td>(626) 818-5230</td>
<td>(714) 969-4958</td>
<td><a href="mailto:cvartanian@a123systems.com">cvartanian@a123systems.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>114 15th Street</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Huntington Beach, California 92648</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td>Chris Villarreal</td>
<td>Regulatory Analyst</td>
<td>California Public Utilities Commission</td>
<td>(415) 703-1566</td>
<td></td>
<td><a href="mailto:crv@cpuc.ca.gov">crv@cpuc.ca.gov</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>505 Van Ness Avenue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>San Francisco, California 94102</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Title</td>
<td>Company</td>
<td>Address</td>
<td>Phone</td>
<td>Fax</td>
<td>Email</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------</td>
<td>------------------------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td><strong>Observer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Josh Wepman</td>
<td>AVP Smart Grid Security Practice Lead</td>
<td>SAIC</td>
<td>209 S. Revena Boulevard, Ann Arbor, MI</td>
<td>(858) 366-2175</td>
<td>(858) 826-9445 Fx</td>
<td><a href="mailto:wepmanj@saic.com">wepmanj@saic.com</a></td>
</tr>
<tr>
<td>Ernest Wohnig</td>
<td>Senior Associate - Energy Security Sector</td>
<td>Booz Allen Hamilton, Inc.</td>
<td>8283 Greensboro Drive, Mclean, VA</td>
<td>(703) 377-1249</td>
<td>(703) 902-3595 Fx</td>
<td><a href="mailto:wohnig_ernest@bah.com">wohnig_ernest@bah.com</a></td>
</tr>
<tr>
<td>Marzia Zafar</td>
<td>Program Manager</td>
<td>California Public Utilities Commission</td>
<td>505 Van Ness Avenue, San Francisco, CA</td>
<td>(415) 703-1997</td>
<td></td>
<td><a href="mailto:zaf@cpuc.ca.gov">zaf@cpuc.ca.gov</a></td>
</tr>
<tr>
<td><strong>NERC Staff</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mark G. Lauby</td>
<td>Vice President and Director of Reliability Assessment and Performance Analysis</td>
<td>North American Electric Reliability Corporation</td>
<td>116-390 Village Boulevard, Princeton, NJ</td>
<td>(609) 452-8060</td>
<td>(609) 452-9550 Fx</td>
<td><a href="mailto:mark.lauby@nerc.net">mark.lauby@nerc.net</a></td>
</tr>
<tr>
<td>Elliott J. Nethercutt</td>
<td>Technical Analyst</td>
<td>North American Electric Reliability Corporation</td>
<td>3353 Peachtree Road, N.E. Suite 600, Atl</td>
<td>(404) 446-2560</td>
<td>(604) 452-9550 Fx</td>
<td><a href="mailto:elliott.nethercutt@nerc.net">elliott.nethercutt@nerc.net</a></td>
</tr>
<tr>
<td>Last Name</td>
<td>First Name</td>
<td>Organization</td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aivaliotis</td>
<td>Sandy</td>
<td>Nexans</td>
<td>38</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>August</td>
<td>JK</td>
<td>CORE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bucciero</td>
<td>Joseph</td>
<td>Bucciero Consulting, LLC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caird</td>
<td>Ken</td>
<td>GE Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calore</td>
<td>James</td>
<td>Public Service Electric and Gas Co.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cappy</td>
<td>Jay</td>
<td>Verizon Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carter</td>
<td>Lawrence</td>
<td>Bonneville Power Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominguez-Garcia</td>
<td>Alejandro</td>
<td>University of Illinois at Urbana-Champaign</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greenfield</td>
<td>Neil</td>
<td>American Electric Power</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gupta</td>
<td>Vinit</td>
<td>Entergy Services, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hanley</td>
<td>Maria</td>
<td>Department of Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hayden</td>
<td>Ernie</td>
<td>Verizon Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ilic</td>
<td>Marija</td>
<td>Carnegie Mellon University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Johnson</td>
<td>Anthony</td>
<td>Southern California Edison Co.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kezunovic</td>
<td>Mladen</td>
<td>Texas A&amp;M University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kotting</td>
<td>Christopher</td>
<td>ThinkSmartGrid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kundur</td>
<td>Deepa</td>
<td>Texas A&amp;M University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lee</td>
<td>Annabelle</td>
<td>EPRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lim</td>
<td>John</td>
<td>Consolidated Edison Co. of New York</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lynd</td>
<td>Donald</td>
<td>Consumers Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manjrekar</td>
<td>Madhav</td>
<td>Siemens Corporate Research</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McCalley</td>
<td>James</td>
<td>Iowa State University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McCarthy</td>
<td>Devin</td>
<td>Canadian Electricity Association</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meeker</td>
<td>Rick</td>
<td>Florida State University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MeynardI</td>
<td>Alessandro</td>
<td>Verizon Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Muller</td>
<td>Nelson</td>
<td>OATI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Myrda</td>
<td>Paul</td>
<td>EPRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rahimi</td>
<td>Farrokh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rinkoski-Spangler</td>
<td>Marie</td>
<td>U.S. Department of Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shastri</td>
<td>Venkat</td>
<td>PCN Technology, Inc</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Souza</td>
<td>William</td>
<td>PJM Interconnection, L.L.C.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stuebing</td>
<td>Gary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thanos</td>
<td>Daniel</td>
<td>GE Digital Energy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tomsovic</td>
<td>Kevin</td>
<td>University of Tennessee (The)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uzunovic</td>
<td>Edvina</td>
<td>The Valley Group (a Nexans Company)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vartanian</td>
<td>Charlie</td>
<td>A123 Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wohnig</td>
<td>Ernest</td>
<td>Booz Allen Hamilton, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wu</td>
<td>Neng</td>
<td>Binghamton University, SUNY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>First Name</td>
<td>Organization</td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------------------------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bossart</td>
<td>Steven</td>
<td></td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cherian</td>
<td>Sunil</td>
<td>Spirae, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ciufi</td>
<td>John</td>
<td>Ciufo and Cooperberg Consulting Ltd.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hedges</td>
<td>Edward</td>
<td>Kansas City Power &amp; Light Co.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miu</td>
<td>Karen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resek</td>
<td>James</td>
<td>KEMA Consulting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Villarreal</td>
<td>Chris</td>
<td>California Public Utilities Commission</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whitaker</td>
<td>Virginia</td>
<td>E.ON U.S.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zdenek</td>
<td>Pamela</td>
<td>BP US Cogens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>First Name</td>
<td>Organization</td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bacik</td>
<td>Sandy</td>
<td>EnerNex Corp</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Booe</td>
<td>Jonathan</td>
<td>North American Energy Standards Board</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DeBlasio</td>
<td>Richard</td>
<td>National Renewable Energy Laboratory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gangopadhyay</td>
<td>Amitabha</td>
<td>National Energy Board</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gordus</td>
<td>Rich</td>
<td>ComEd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kalisch</td>
<td>Richard</td>
<td>Midwest ISO, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wepman</td>
<td>Josh</td>
<td>SAIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>First Name</td>
<td>Organization</td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------------------------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bochman</td>
<td>Andy</td>
<td>IBM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Howe</td>
<td>Gavan</td>
<td>Howe Brand Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Katz</td>
<td>Jeffrey</td>
<td>IBM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mertz</td>
<td>Michael</td>
<td>PNM Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overman</td>
<td>Thomas</td>
<td>Boeing Defense, Space &amp; Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vittal</td>
<td>Vijay</td>
<td>Arizona State University</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>