NSTB
National SCADA Test Bed
enhancing control systems security in the energy sector

Smart Grid Security - Procurement

SANS
Process Control &
SCADA
SECURITY SUMMIT 2010

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability
Agenda

- National SCADA Test Bed
- Smart Grid Investment Grants
- Status of Technology
- Ubiquitous Technology
- Threat Actors and Motivations
- Research Questions Remain
- Mitigations
  - OpenSG: AMI-Sec ASAP-SG
  - Procurement Language for AMI Wireless
  - NIST standards efforts
DOE National SCADA Test Bed Program

Purpose: Support industry and government efforts to enhance cyber security of control systems in energy sector

...established 2003

Key Program Areas

- Assess energy control systems vulnerabilities/ develop mitigation recommendations
- Outreach and awareness
- Integrated Risk analysis
- Develop advanced, secure control systems technologies

“...the only reliable way to measure security is to examine how it fails”

Bruce Schneier, Beyond Fear
Smart Grid Investment Grants Awardees

- AMI: $19,786,501.00
- Computer Systems: $818,242,729.00
- Distribution: $32,402,210.00
- Transmission: $254,260,747.00
- Equipment Manufacturing: $147,990,985.00
- Crosscutting: $1,978,501,000.00

Total: $2,150,465,323.00
Smart Grid Infrastructure Grants

- **DE-FOA-0000058**
  - 431 applicants totaling $24.6B
  - 100 awarded totaling $3.4B, Large and small utilities
  - 14 Entities award limited authority funds $2.2B obligated

- Few utilities didn’t apply
  - No renewable portfolio standard, Low energy rates, Weak competition, complex integration of applications

- Negotiation Phase
  - All costs invoiced and paid September 30, 2015
  - Davis-Bacon prevalent wage requirements
  - Made in America rule
  - Property Encumbrances
  - Questions on taxes
  - State regulatory approval rate cases
  - Project reports, build metrics, impact metrics
AMI Security Challenges

Systems are vulnerable

• Access Points everywhere
• Access point physical security
• Complex networks provides more opportunities for attacks
• Distribution systems outside of regulatory cyber standards
• Information readily available
• Wireless Communications
• Multiple vendors

4.2. The following are exempt from Standard CIP-002:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
AMI Security Challenges continued

• Integration of applications never before integrated
  – Distribution systems integrated with T&G
  – Legacy applications normally isolated from other networks
  – Known vulnerabilities in legacy SCADA/EMS
  – Known vulnerabilities in AMI
  – Integration code will have vulnerabilities

• Onus on Owners and Operators to implement security
  – Operators have a better understanding of security needs

• Finding and retaining talent in cyber security problematic

---

Billions to be spent on smart grid cybersecurity | Security - CNET...
Feb 4, 2010 ... Utility companies around the world will spend $21 billion by 2015 to improve cybersecurity for the world’s electrical smart grid, ...
news.cnet.com/3600-1099_3-10447430-83.html - Cached

Power Up on Smart Grid Cyber Security - The Source - WSJ
Feb 25, 2010 ... Pike Research, a clean-tech market research firm, expects the global smart grid cyber security market to grow to $4.1 billion in 2013 at a ...
blogs.wsj.com/source/2010/02/...smart-grid-cyber-security/.../article/ - Cached

Feds Will Spur Smart Grid Cyber-Security Investment Growth to $21...
Feb 9, 2010 ... The Smart Grid Cyber Security Report, conducted courtesy of Pike Research, ...
sector career opportunities in GovTech’s new jobs section. ...
www.govtech.com/gt/articles/744630 - Cached

Utilities to bolster smart grid cybersecurity |...
Feb 8, 2010 ... Pike's Smart Grid Cyber Security report identifies five areas of focus for utility...
AMO Observations

- Few Vendors provide end to end solutions without changing technologies
- Fewer installations will be able to afford end to end solutions
  - Integration with legacy systems is the norm
  - Multiple generations of meters or head end equipment common
- AMI architectures provide for a target rich environment
- Owners and Operators customer privacy and fraud savvy
- Large asset owner IT networks being pinged 3 million times a day from foreign IP address
- AMI data will be used in IT Billing and Control Operations networks
Meter Vulnerabilities Found by Many Sources

AMI Embedded Systems

- Insecure data busses and serial connections
  - C12.22 bus
  - Data Capture, Injection (both directions)
    - Radios
    - MCU's
- Stealing/Replacing Keys In Memory
  - Network Encryption
  - Authentication and CA keys
- Blown JTAG Fuse Isn't Enough
  - Third-party labs remove top/allow microscopic access to chip
- Firmware-level vulnerabilities similar to x86 systems
- It’s the Latch!

Topics for Today

- Bootloader Timing Attacks
  - to extract firmware.
- Efficient Jamming
  - by use of radio test modes.
- Bus Tapping
  - to extract network keys.
- Stack Overflows
  - to execute arbitrary machine code.

Matt Carpenter – InGuardian – Presented at SANS SCADA 2009

Travis Goodspeed University of Tennessee – Presented at S4
**Research Questions**

- Number of meters opened to impact BPS?
- What is the scalability of architectures?
- What is the impact of cellular as a backhaul?
- What is the impact of complex control schemes?
- What is the impact of these schemes being used on multiple vendor/communications platforms?
- Will islanding make the grid more unstable due to regional interests taking priority over the BPS?
**AMI System Security Requirements**

<table>
<thead>
<tr>
<th>V1.01</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAP</td>
</tr>
</tbody>
</table>

**Executive Summary**

This document provides the utility industry and vendors with a set of security requirements for Advanced Metering Infrastructure (AMI). These requirements are intended to be used in the procurement process, and represent a superset of requirements gathered from current cross-industry accepted security standards and best practice guidance documents.

**UtiliSec Working Group**

**Motivation:**
- Part of a utility-led, electric power industry community effort (UCAIug) to define a common set of requirements for the procurement of new technologies

**Status:**
- Suite of 4 deliverables completed in 2008
  - AMI Security Risk Assessment
  - AMI System Security Requirements (incorporates Architectural Description)
  - AMI Security Component Catalog
  - AMI Security Implementation Guide
- AMI System Security Requirements document ratified December, 2008 ("1.0")

**Current Participation:**
- 200+ Subscribers to Listserv across 8 countries and 4 continents
- More than a dozen major North American utilities actively engaged
NIST Smart Grid

1. Cyber Security Strategy
2. Logical Architecture 18 (23) Logical Interface Categories mapped to DHS’s Catalog of Requirements
3. High Level Security Requirements
4. Privacy
5. Standards
6. R&D Themes
Standards: References

Catalog of Control Systems Security: Recommendations for Standards Developers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.17.2</td>
<td>Continuous Improvement</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.17.3</td>
<td>Monitoring of Security Policy</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.17.4</td>
<td>Best Practices</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.17.5</td>
<td>Security Accreditation</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.17.6</td>
<td>Security Certification</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.1</td>
<td>Risk Assessment Policy and Procedures</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2.18.2</td>
<td>Risk Management Plan</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2.18.3</td>
<td>Certification, Accreditation, and Security Assessment Policies and Procedures</td>
<td>X</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.4</td>
<td>Security Assessments</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.18.5</td>
<td>Control System Connections</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.18.6</td>
<td>Plan of Action and Milestones</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.7</td>
<td>Continuous Monitoring</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.8</td>
<td>Security Categorization</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.9</td>
<td>Risk Assessment</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2.18.10</td>
<td>Risk Assessment Update</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2.18.11</td>
<td>Vulnerability Assessment and Awareness</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.18.12</td>
<td>Identify, Classify, Prioritize, and Analyze Potential Security Risks</td>
<td>----</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>----</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

January 2008
Enhancing Control Systems Security in the Energy Sector

Trend: Compliance vs Measurements

Consensus Audit Guidelines

Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Additional Critical Controls (not directly supported by automated measurement and validation):

16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps
Smart Grid Infrastructure Security Requirements

Large Asset Owners are concerned and being proactive
Up front security requirements
Assumptions that address common security issues

Assumptions for AMI Security

- **Standards based security and functionality**
  - No “security by obscurity” – i.e., using proprietary code and expect it to be secure just because the hackers have not seen it
- **Physical compromise of devices will be common place**
- **Back office will be compromised**
- **Focus on protecting sensitive information and commands – encryption and digital certificates**
- **Defense in depth – Layers of security throughout**
- **North American Electric Reliability Council’s Critical Infrastructure Protection (NERC CIP) standards must be evaluated at all layers of architecture**

Example of asset owner assumptions

Mid to Small Asset Owners do not have the cyber security staff to design security into their AMI networks
Securing AMI Networks

Wireless Procurement Language

DOE-OE NSTB sponsored Wireless Procurement Language in Support of AMI Security August 2009

- 802.11
- WiMAX
- Wireless Mesh
- WirelessHART
- ZigBee
- Bluetooth
- Mobile Radio
- Cellular
- Microwave and Satellite
## Mitigations Procurement

<table>
<thead>
<tr>
<th>Issue</th>
<th>Wireless Procurement</th>
<th>Procurement</th>
</tr>
</thead>
</table>
| Rogue Node Mesh Networks                   | 3.3 Mesh - nodes basic attack test data shall show malformed packet injections do not cause the wireless meshed network device to crash, hang or otherwise malfunction  
4.3 HART - vendor shall provide security devices such as passwords or security codes to protect the device from unauthorized modifications or use  
1.3 802.11 - WiFi nodes can distinguish jamming from channel saturations and provide operational alerts  
2.3 WiMAX - document the range of the WiMAX subscriber station, power requirements and the designated frequency of operation for each device | 2.4.3 Hardware Configuration – configure network devices to limit access to/from specific locations                                                                                                               |
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Procurement Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Code</td>
<td>5.1.3 Coding Practices – provide results of code review</td>
</tr>
<tr>
<td></td>
<td>6.2.3 Problem Reporting – notify purchaser of all problems and remediation steps regardless of origin</td>
</tr>
<tr>
<td></td>
<td>6.1.3 Flaw Remediation – document written flaw remediation process and provide updates and/or workarounds to mitigate</td>
</tr>
</tbody>
</table>
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Wireless Procurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mid Distance to Backhaul</td>
<td>7.3 Mobile Radios – vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT</td>
</tr>
<tr>
<td>Communications Control</td>
<td>8.3 Cellular – the vendor shall perform an interference rejection test and supply the results with an explanation of the results</td>
</tr>
<tr>
<td></td>
<td>9.3 Microwave Satellite - the vendor shall allow and recommend alarm settings in accordance to the needs of the system</td>
</tr>
</tbody>
</table>
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Wireless Procurement</th>
<th>Procurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak Authentication</td>
<td>5.3 Zigbee - vendor shall clearly identify security devices and methods to change from the vendor-configured or manufacture default conditions</td>
<td>4.3.3 Authentication Policy – vendor will not store passwords electronically or provided in documentation</td>
</tr>
<tr>
<td></td>
<td>4.2.3 Session Management provide strongest encryption method commensurate with the technology platform and response time constraints</td>
<td>4.5.3 Role Based Access Control – shall not escalate privileges, adhere to least privileged</td>
</tr>
<tr>
<td>Lack of Authorization</td>
<td>1.3 802.11 identify the configuration control options that enable varying of the security level of the device</td>
<td>4.5.3 Role Based Access Control – shall not escalate privileges, adhere to least privileged</td>
</tr>
</tbody>
</table>
Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Procurement Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor Chip Sets</td>
<td>5.1.3 Coding Practices – vendor shall share practices and standards applied to vendor written control system software, including firmware used</td>
</tr>
<tr>
<td></td>
<td>6.2.3 Problem Reporting – vendor shall provide auditable history of flaws including the remediation steps taken</td>
</tr>
<tr>
<td>Too Flexible Configurations – Meters and Head end components</td>
<td>9.4.3 Sensors Actuators Meters – provide physical and cyber security features e.g. authentication, encryption access control, logging, event monitoring and alarming</td>
</tr>
<tr>
<td></td>
<td>9.3.5 PLC – provide methods to verify/change settings from vendor configured or manufacture default conditions</td>
</tr>
<tr>
<td></td>
<td>2.4.3 Hardware Configuration – document all disabled or removed ports, drives and other removable media devices</td>
</tr>
</tbody>
</table>
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Procurement Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Maintenance Access</td>
<td>10.1.3 Remote Access – shall not permit user’s credentials transmitted in clear text</td>
</tr>
<tr>
<td></td>
<td>10.1.3 Remote Access – shall not adversely affect connectivity, latency, bandwidth, response time and throughput</td>
</tr>
<tr>
<td></td>
<td>4.1.3 Disable Accounts – disable all vendor owned accounts or negotiate account ownership with the Purchaser</td>
</tr>
</tbody>
</table>

![Diagram of network security setup](image)
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Wireless Procurement</th>
<th>Procurement Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abandon Components</td>
<td>5.3 Zigbee – state the low rate wireless personal area network replacement options 6.3 Bluetooth – provide test data since all implementations of Bluetooth are not the same</td>
<td>4.7.3 Separation Agreements – return all sensitive data when the vendor is no longer able to maintain control of the purchaser’s products</td>
</tr>
<tr>
<td>Integration with Customer Information Systems</td>
<td>2.3 WiMAX - document the range of the WiMAX subscriber station, power requirements and the designated frequency of operation for each device 5.3 Zigbee – define interoperability limits for low rate wireless personal area networks</td>
<td>4.7.3 Separation Agreements – notify purchaser when key employee leaves position and prohibit disclosure of information 5.1.3 Coding Practices – provide documentation of coding practices used in the development and delivered software 6.2.3 Problem Reporting – report initial action plan within 24 hours of submitting a problem report 6.1.3 Flaw Remediation – verify changes to core system, logic or configuration that new vulnerabilities are not introduced</td>
</tr>
</tbody>
</table>
## Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Procurement Specification</th>
</tr>
</thead>
</table>
| Physical Access          | 11.1.3 Physical Security – provide lockable or locking enclosures for components  
                        | 2.4.3 Hardware Configuration - disconnect or disable all unneeded communications ports and remove media devices or provide engineered barriers                                                                                                           |
| White Listing            | 3.1.3 Firewalls – provide explicitly identified rule sets  
                        | 2.2.3 Host-based Intrusion Detection – identify static file names, dynamic file patterns and alarm on unauthorized code execution  
                        | 4.4.3 Account Auditing and Logging – ensure audit logging does not adversely impact system performance requirements  
                        | 3.3.3 Network Intrusion Detection – provide traffic profiles, expected communication paths and utilization boundaries                                                                                                    |

**Allowed Network Flows**

<table>
<thead>
<tr>
<th>Host</th>
<th>Host</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>TCP 80</td>
</tr>
<tr>
<td>C</td>
<td>D</td>
<td>TCP 123</td>
</tr>
</tbody>
</table>

Alert on all other flows
### Mitigations Procurement continued

<table>
<thead>
<tr>
<th>Issue</th>
<th>Wireless Procurement</th>
<th>Procurement Specification</th>
</tr>
</thead>
</table>
| HAN     | 5.3 Zigbee – source node authentication shall be implemented  
6.3 Bluetooth - vendor shall provide detailed information on the communications (including protocols) required for the Bluetooth-enabled device to communications with the control network and the types of network devices with which it can communicate |  
| Scalable| 1.3 802.11 – analyze potential radio frequency interference, determine adequate wireless LAN coverage and set configurations parameters properly | 9.4.3 Sensors, Actuators and Meters – verify security feature does not adversely affect connectivity, latency, bandwidth, response time and throughput |
Questions Asset Owners Should Ask

- What are the known vulnerabilities with components, networks and applications?
- Has the code reviewed by an independent security expert?
- What is the capacity limitations with the architecture?
- Have these applications/components been integrated before? and if so was a vulnerability assessment for security completed?
- Is there a white list of network communications/applications available?
- Is there deep packet inspection for untrusted communications and context checking available?
- What are the controls of updates and maintenance access to components/applications?
Trend: Risk vs Resilience

Resilience

Change is constant
Everything breaks
Human Error
Machine Failure
Adaptive Capability vs Brittleness and Optimization

Resilient systems can restructure when faced with change and failures
With no adaptation process, systems will fail when faced with change

Traditional Risk
Risk = Threat x Vulnerability x Consequence
Actuation tables based on past
Summary of Smart Grid Activities

DOE-OE/NSTB work
- Smart Grid Systems – Current Cyber Security Issues (April 2009)
- NSTB Substation Automation Evaluation Report (October 2009)
- Advance Meter Infrastructure (AMI) Security Accelerated Program (ASAP)
  - AMI Wireless Procurement Specification (August 2009)
  - Open Smart Grid User Group member osgug.ucaiug.org
- Phase 2 AMI Cyber Security Vulnerability Assessment (FY10)
- AMI Onsite Cyber Security Vulnerability Assessment (FY10)
- North American SynchroPhasor Initiative (NASPI)
  - Data and Network Management Task Team
- Outreach on smart grid cyber security
  - SANS, NARUC, ALCA, GridWeek, GridWise Architecture Council
- Smart Grid R&D Multi-Year Plan 2010-2014 – provided requirements

Strategic Work For Others
- AMI Cyber Security Vulnerability Assessment – Itron Phase 1 (2009)
Contacts

Idaho National Laboratory
Rita Wells
(208) 526-3179

National SCADA Test Bed
Hank Kenchington
Henry.kenchington@hq.doe.gov
Carol Hawk
Carol.hawk@hq.doe.gov

http://www.oe.energy.gov/controlsecurity.htm