U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery and Energy Reliability

Smart Grid Cybersecurity Lessons Learned

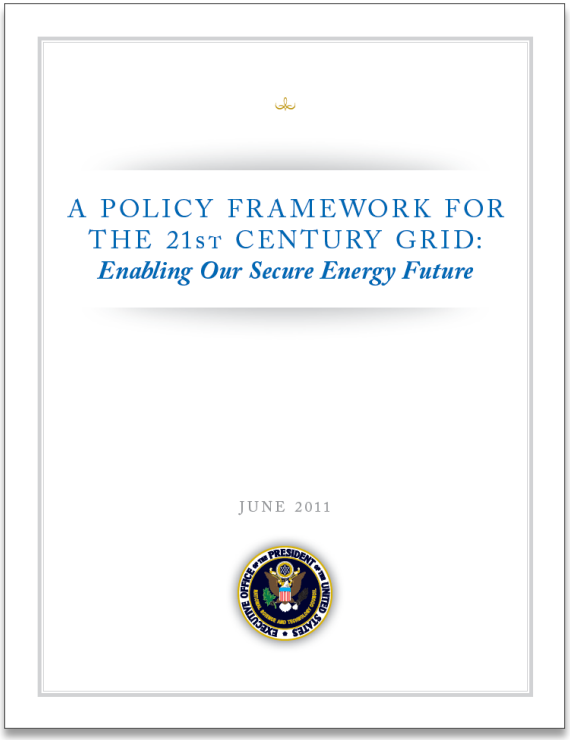
From More than 11 Million Smart Meters Deployed

Hank Kenchington
Deputy Assistant Secretary
Office of Electricity Delivery and Energy Reliability

Grid Modernization: A National Energy Priority

Energy Infrastructure & Security Act of 2007 (EISA)
Title XIII – SMART GRID

"It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth…"



"We'll fund a better, smarter electricity grid and train workers to build it -- a grid that will help us ship wind and solar power from one end of this country to another."

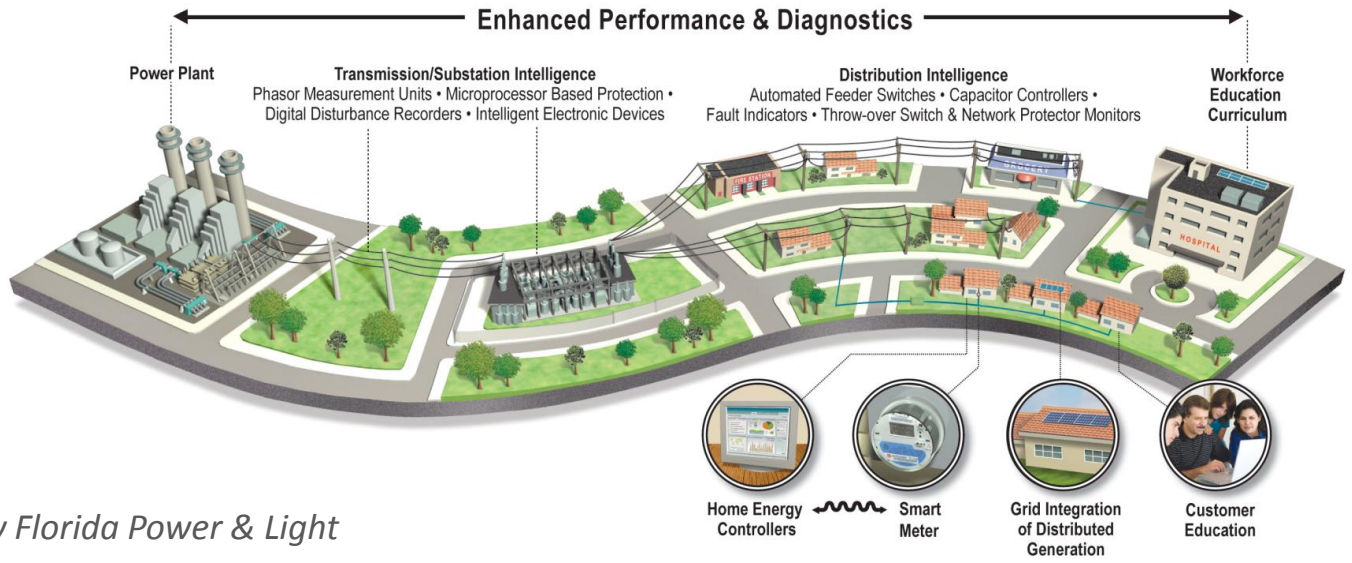
President Barack Obama

2

Seven Principal Characteristics of a Smart Grid

1. Empowers consumers
2. Accommodates all generation and storage
3. Enables new products, services and markets
4. Increases power quality for our connected economy
5. Optimizes asset use and operates efficiently
6. Anticipates and responds to disturbances
7. Operates resiliently against attack and natural disaster

Smart Grid Requires Seamless, SECURE Communications Across Multiple Interconnected Domains and Platforms

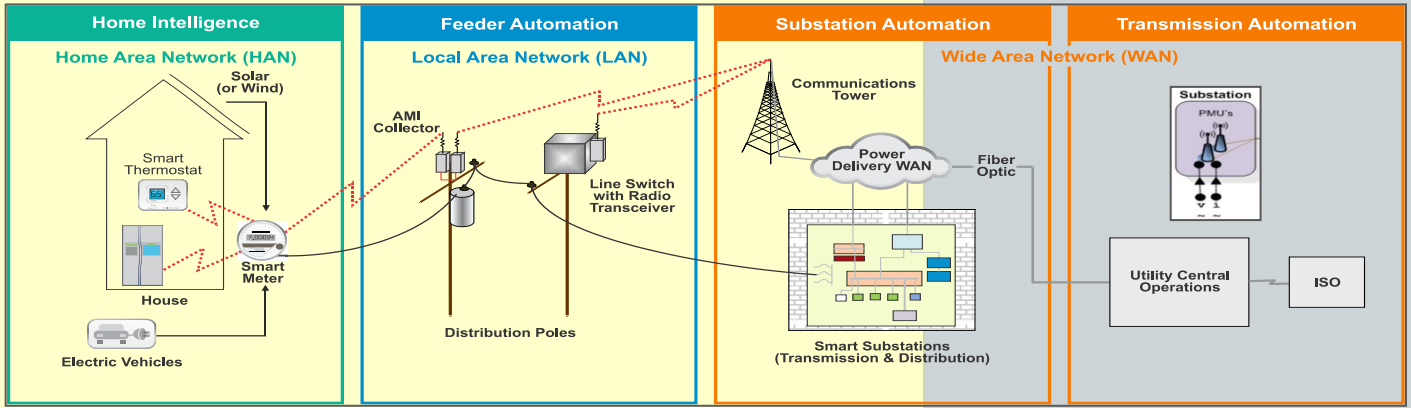


Courtesy Florida Power & Light

2009: No cybersecurity standards for distribution system or home area networks

2005: Mandated cybersecurity standards for bulk power system

Generic Smart Grid Communications Architectures



2009 Recovery Act Provided $4.5 billion for Grid Modernization

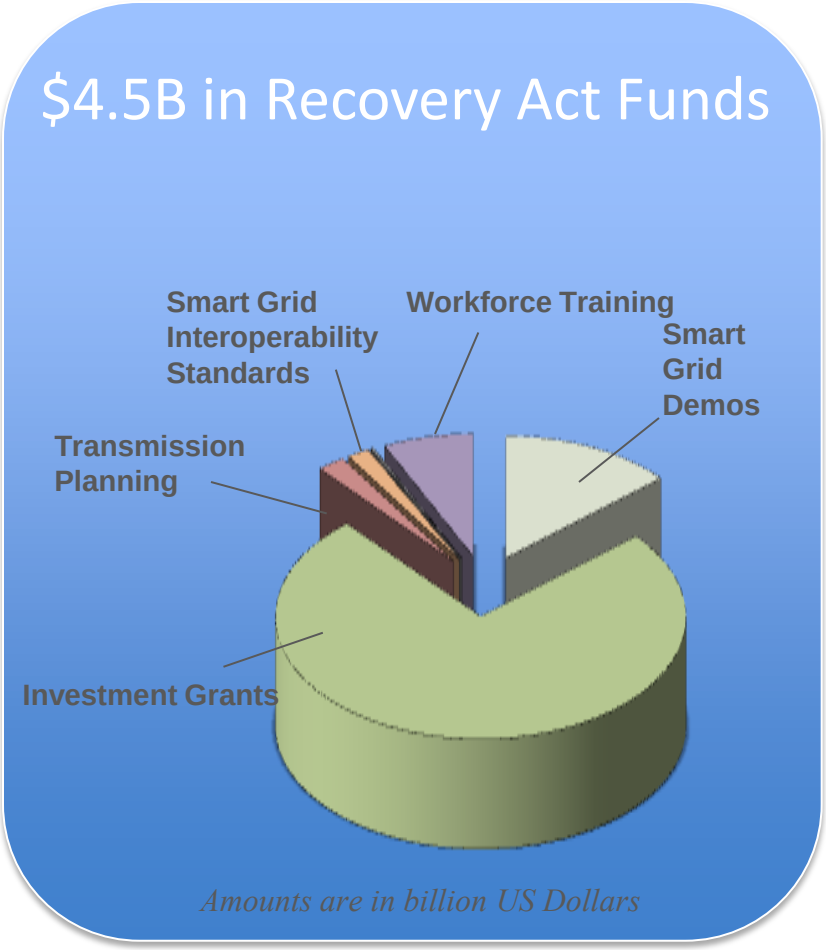
Programs created by statute:

American Recovery and Reinvestment Act of 2009

- $3.4 billion - Smart Grid Investment Grants (SGIG)*
- $620 million - Smart Grid Regional Demonstrations (SGDP)*
- $100 million - Workforce Training
- $80 million - Interconnection-wide Transmission Planning and Resource Analysis
- $12 million - Interoperability Standards

Additional OE Recovery Act Initiatives:

- $44 million-Technical Assistance to States
- $10 million-Local Energy Assurance Planning



Source: www.smartgrid.gov

**Originally authorized by the Energy Infrastructure Security Act 2007, EISA 1306 and EISA 1304*

SMARTGRID.GOV
RECOVERY ACT SMART GRID PROGRAMS

SGIG Program Objectives

- ***Accelerate deployment*** of smart grid technologies across the transmission and distribution system and empower consumers with information so they can better manage their electricity consumption and costs
- ***Measure the impacts and benefits*** of smart grid technologies to reduce uncertainty for decision makers and attract additional capital and further advance grid modernization
- Accelerate the development and deployment of ***effective cybersecurity protections and interoperability standards*** for smart grid technologies and systems

Significant investments required to modernize US grid

SGIG projects seek to *accelerate* industry investment

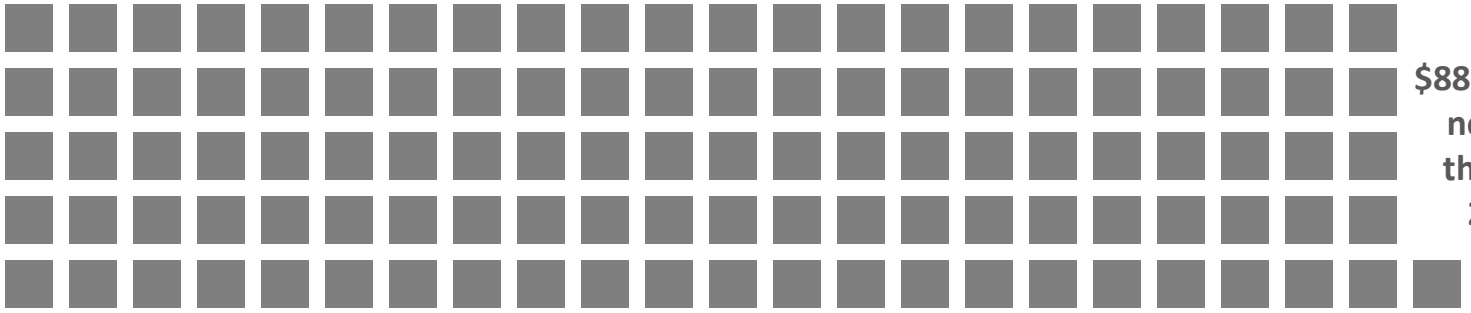
ARRA SGIG — **$7.9 billion with cost share to be spent through 2015**

EPRI Estimate

$338 - $476 billion needed through 2030

EPRI. Estimating the costs and benefits of the smart grid: A preliminary estimate of the investment requirements and the resultant benefits of a fully functioning smart grid. EPRI, Palo Alto, CA; 2011.

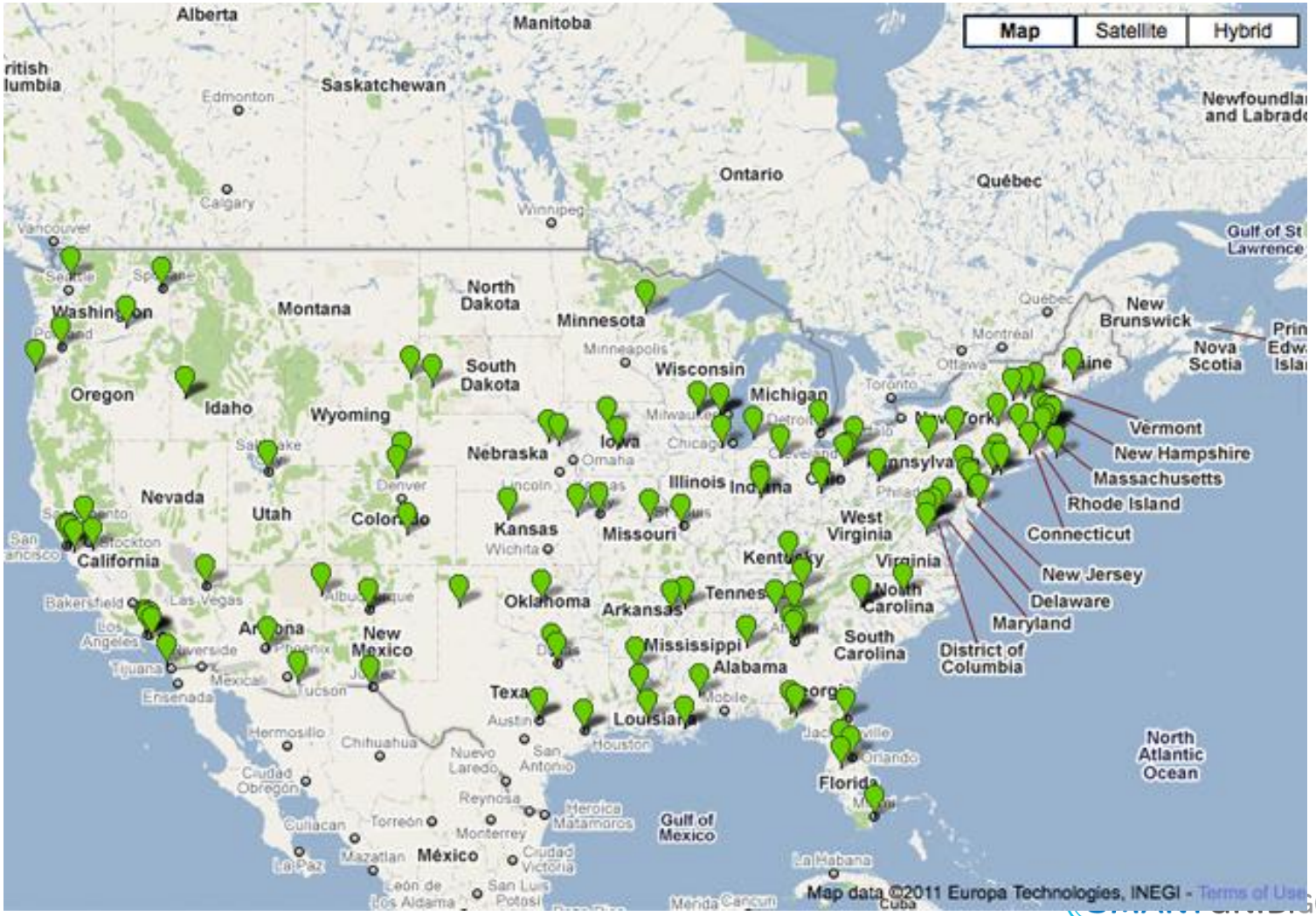
Brattle Group Estimate



$880 billion needed through 2030

Chupka, M.W. Earle, R., Fox-Penner, P., Hledik, R. Transforming America's power industry: The investment challenge 2010 – 2030. Edison Electric Institute, Washington D.C.,: 2008.

+$7.9 Billion in Smart Grid Assets Now Being Deployed thru SGIG



SGIG Project Expected Benefits

	Total Funds	Key Installations by 2015	Expected Benefit
	***Transmission***		
	$580 million	**800** phasor measurement units	Real-time voltage and frequency fluctuations visible across the system
	***Distribution***		
	$1.96 billion	**7,500** automated switches **18,500** automated capacitors	Outage management. Improved reliability, VAR control
	***AMI***		
	$3.96 billion	**15.5 million** smart meters	Operational savings: fewer truck rolls, automated readings, reduced outage time
	***Customer Systems***		
	$1.33 billion	**>222,000** direct control devices **>192,000** thermostats **>7,000** in-home displays	Increased customer control; reduced peak demand

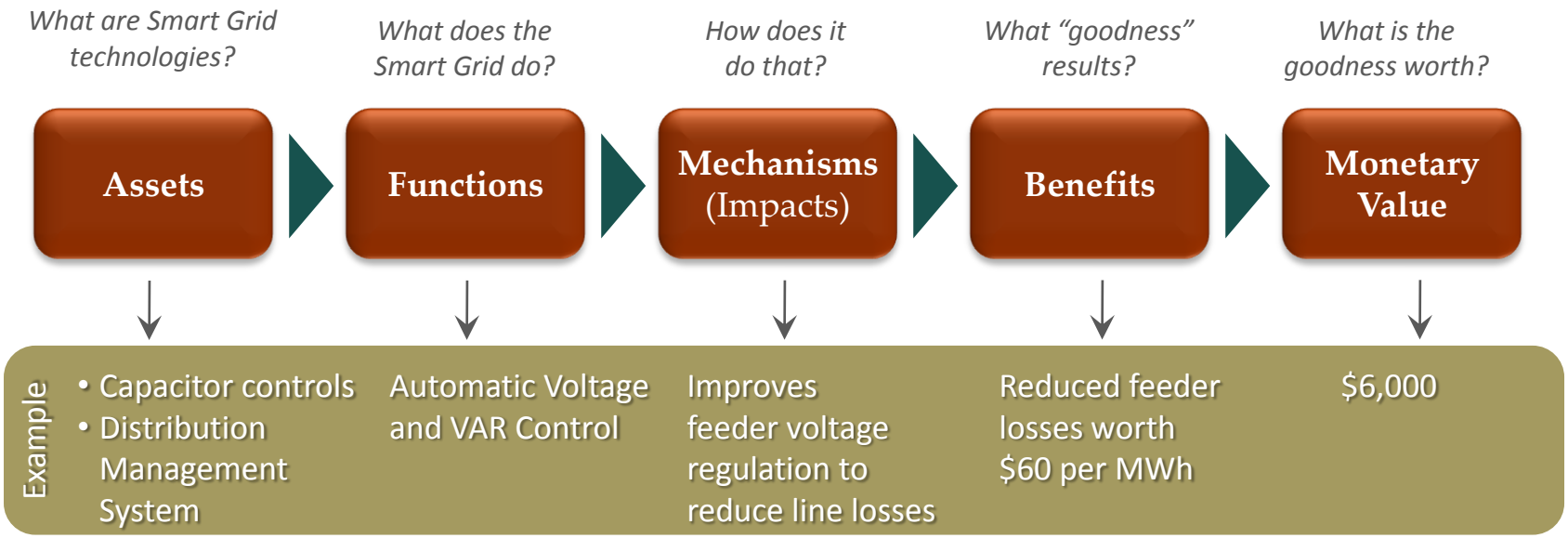
SMARTGRID.GOV
RECOVERY ACT SMART GRID PROGRAMS

SGIG Applications and Benefits Matrix

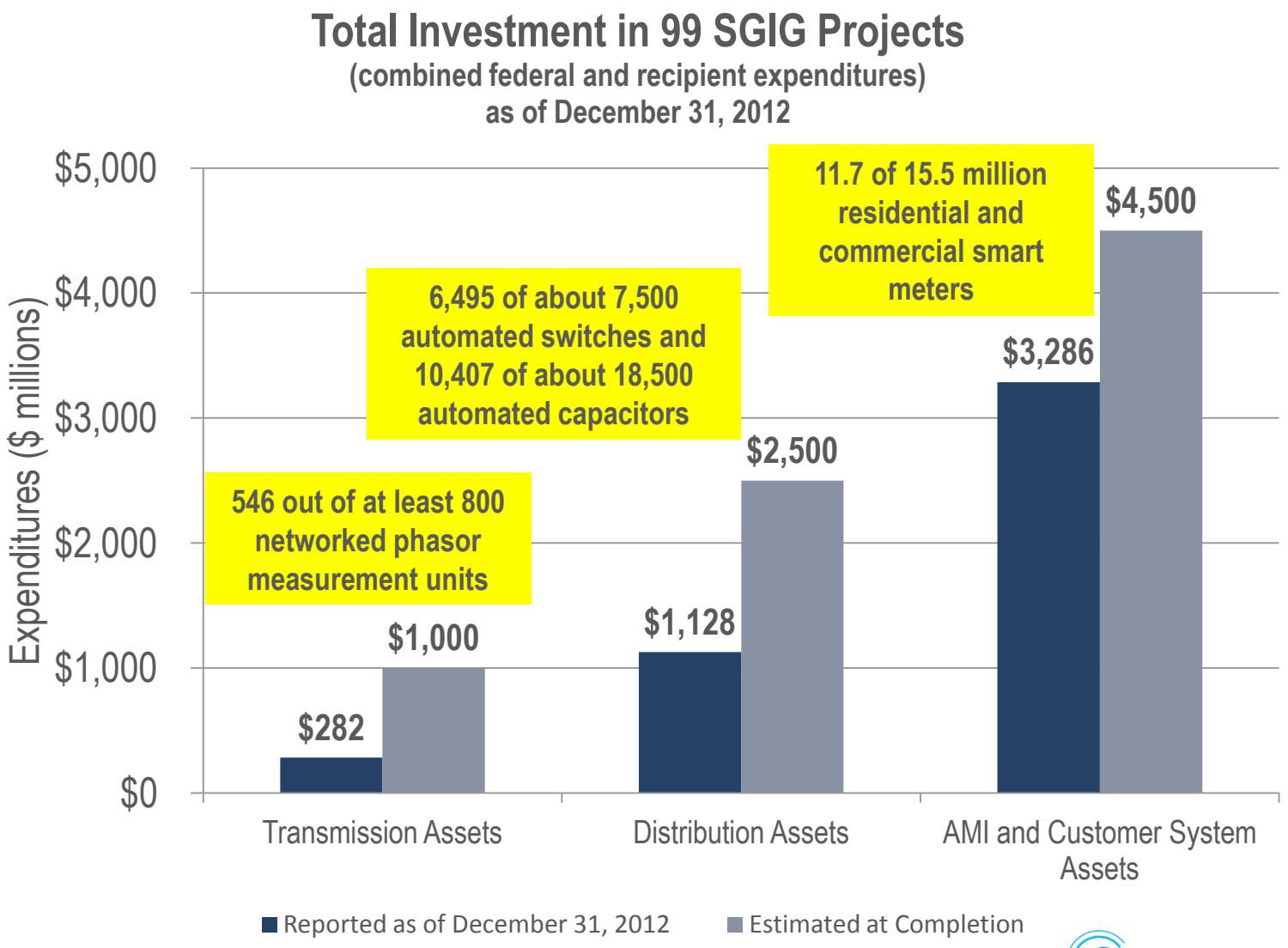
Benefits	Smart Grid Technology Applications					
	Consumer-Based Demand Management Programs (AMI-Enabled)	**Advanced Metering Infrastructure (AMI) Applied to Operations**	**Fault Location, Isolation and Service Restoration**	**Equipment Health Monitoring**	**Improved Volt/VAR Management**	**Synchrophasor Technology Applications**
	• Time-based pricing • Customer devices (information and control systems) • Direct load control (does not require AMI)	• Meter services • Outage management • Volt-VAR management • Tamper detection • Back-Office systems support (e.g., billing and customer service)	• Automated feeder switching • Fault location • AMI and outage management	• Condition-based maintenance • Stress reduction on equipment	• Peak demand reduction • Conservation Voltage Reduction • Reactive power compensation	• Real-time and off-line applications
Capital expenditure reduction – enhanced utilization of G,T & D assets	✔			✔	✔	✔
Energy use reduction	✔	✔	✔		✔	✔
Reliability improvements		✔	✔	✔		✔
O&M cost savings		✔	✔	✔		
Reduced electricity costs to consumers	✔				✔	
Lower pollutant emissions	✔	✔	✔		✔	✔
Enhanced system flexibility – to meet resiliency needs and accommodate all generation and demand resources	✔	✔	✔	✔	✔	✔

Building the Business Case through Sound Metrics and Analysis

Correlating technology, enhanced grid function and capability, costs, and benefits



SGIG – Making Progress



SMARTGRID.GOV
RECOVERY ACT SMART GRID PROGRAMS

OGE Sees Peak Demand Reductions from AMI and Pricing Strategies

Oklahoma Gas and Electric

- 765k customers, 778MW gen
- Study: 2-year demand response study of 6,000 customers in dynamic rate programs with IHDs and "smart" thermostats

Results:

- ➔ Up to 30% reduction in demand during peak periods (variable peak pricing rates).
- ➔ The SmartHours program saved an average of $150 per household in summer 2011.
- ➔ 1.3kw average peak demand reduction
- ➔ If benefits continue during wider rollout, OG&E will defer construction of a natural-gas-fired peaking plant

Distributed Automation Improved Reliability at FPL

Florida Power & Light

- 4.6 million customers, 70k miles power lines
- Study: Installed 230 automated feeder switches on 75 circuits in Miami area that sense and communicate data about current, voltage, phase, fault occurrence, and switch position to the DMS

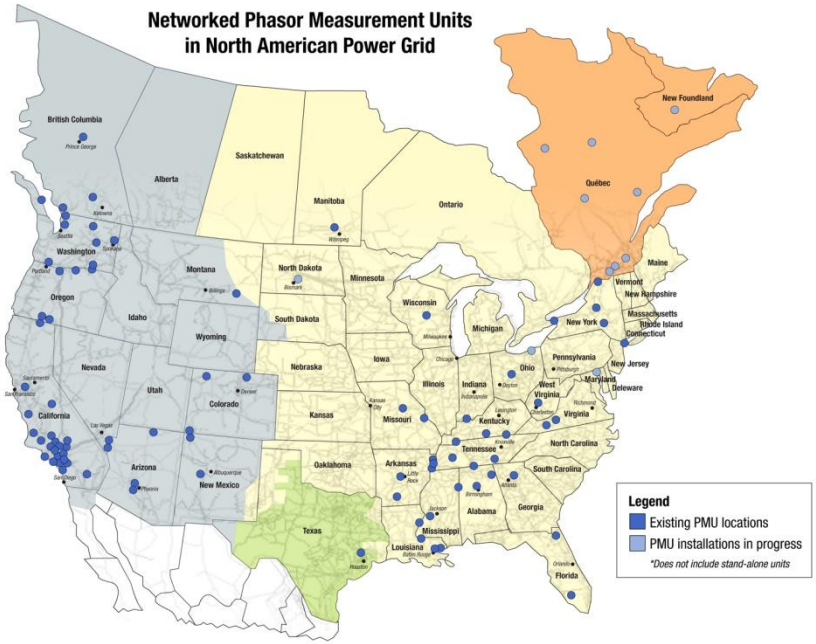
Results:

- ➔ SAIDI improved 24%. The average outage duration for the six month observation period decreased from 72.3 minutes to 54.6 minutes.
- ➔ SAIFI improved 40%. The average outage frequency during the six month observation period decreased from 1.03 to 0.61 occurrences.
- ➔ MAIFI improved 34.9%. The average momentary interruption frequency decreased from 12.6 to 8.2 occurrences.

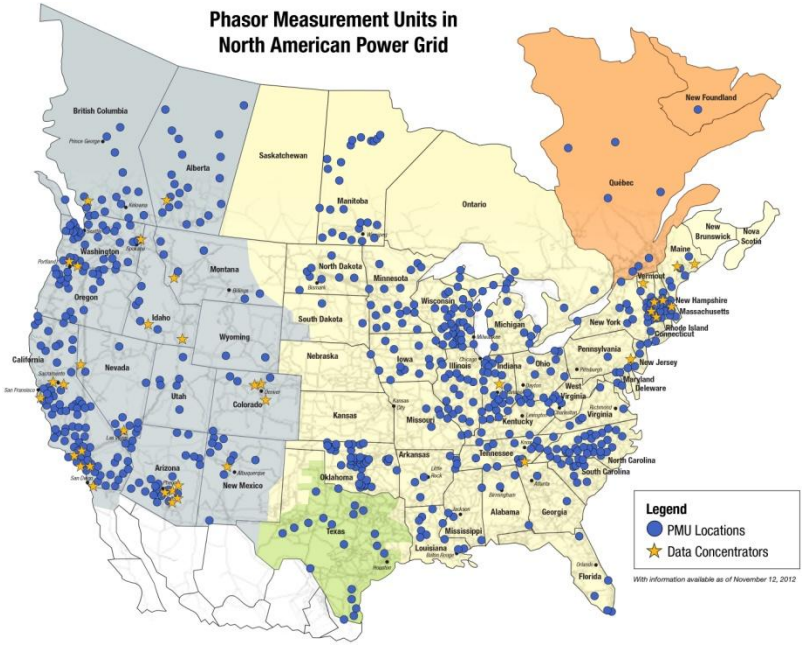
North American SynchroPhasor Initiative

DOE and NERC are working together closely with industry to enable wide area time-synchronized measurements that will enhance the reliability of the electric power grid through improved situational awareness and other applications

April 2007



November 2012



"Better information supports better - and faster - decisions."

NASPI North American SynchroPhasor Initiative

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Making Progress: 4 Impact Reports Issued

- Comprehensive project information
- Progress Reports
- 4 new **Impact Reports** showcasing results and benefits

Available at:

SMARTGRID.GOV

SMARTGRID.GOV
RECOVERY ACT SMART GRID PROGRAMS

SGIG Cyber Security Plan (CSP) Requirements

Build-in security!!!

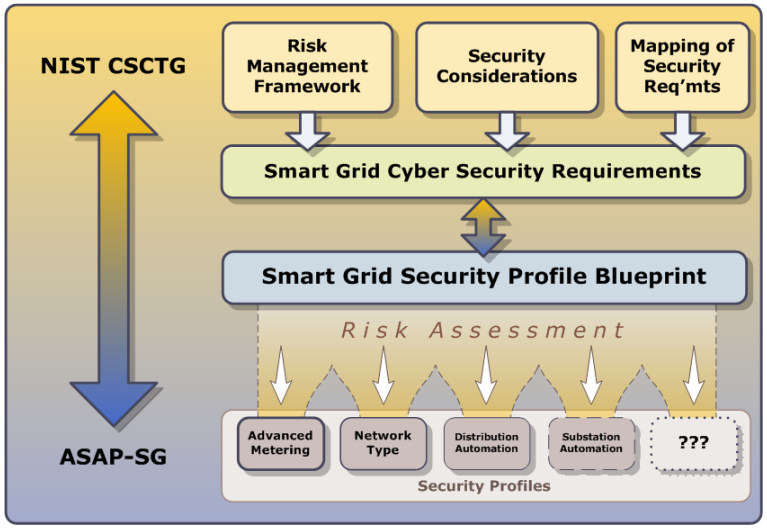
- Evaluate risks and how they will be mitigated at each stage of the project lifecycle
- Criteria for vendor and device selection
- Summarize relevant cybersecurity standards and/or best practices that will be followed
- Upgradeability of components and systems
- How the project will support emerging standards
- Evidence to demonstrate and validate the effectiveness of the cybersecurity controls
- Accountability

Advanced Security Acceleration Project - Smart Grid (ASAP-SG)

- **Industry-government collaboration initiated in 2008 to accelerate development of security requirements and standards for smart grid - completed (smartgridipedi.org):**
  - AMI Security Profile v2.0
  - Third Party Data Access Security Profile v1.0
  - Distribution Management Security Profile v1.0
  - Wide-Area Monitoring, Protection, and Control (Synchrophasor) Security Profile (Draft) v0.08
  - Security Profile Blueprint v1.0
  - How a Utility Can Use ASAP-SG Security Profiles (White Paper)

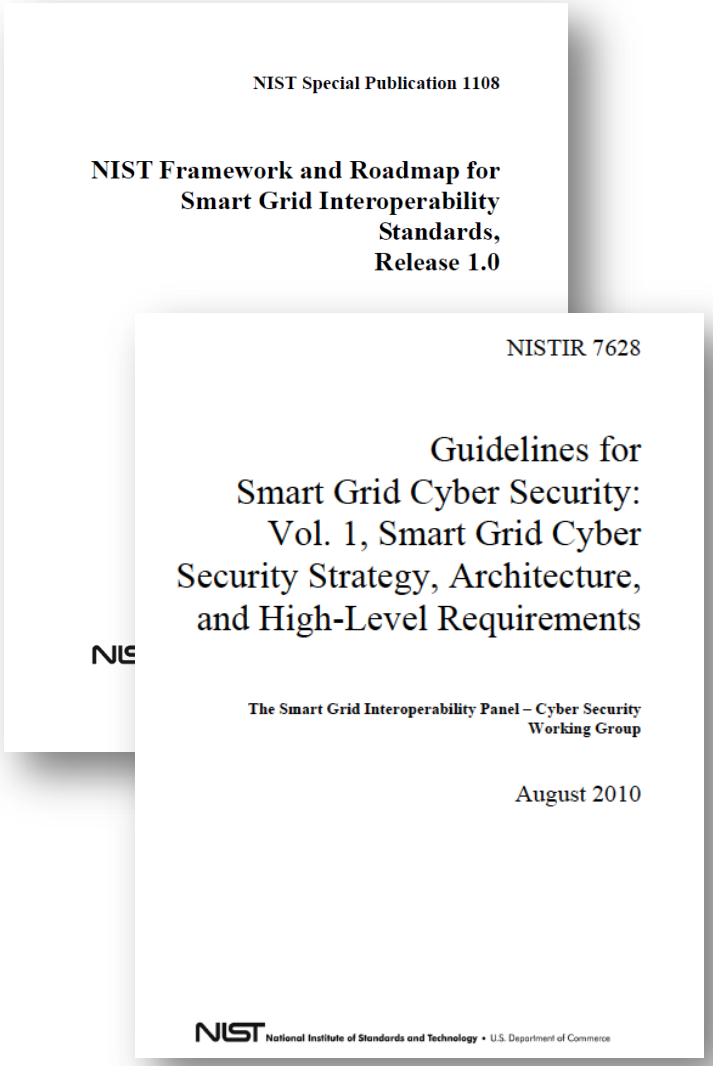
- **Supported development of NISTIR 7628**

- **Industry participants:**
  - American Electric Power
  - Con Edison
  - Consumers Energy
  - Florida Power & Light
  - Southern California Edison
  - Oncor
  - BC Hydro
  - EPRI



18

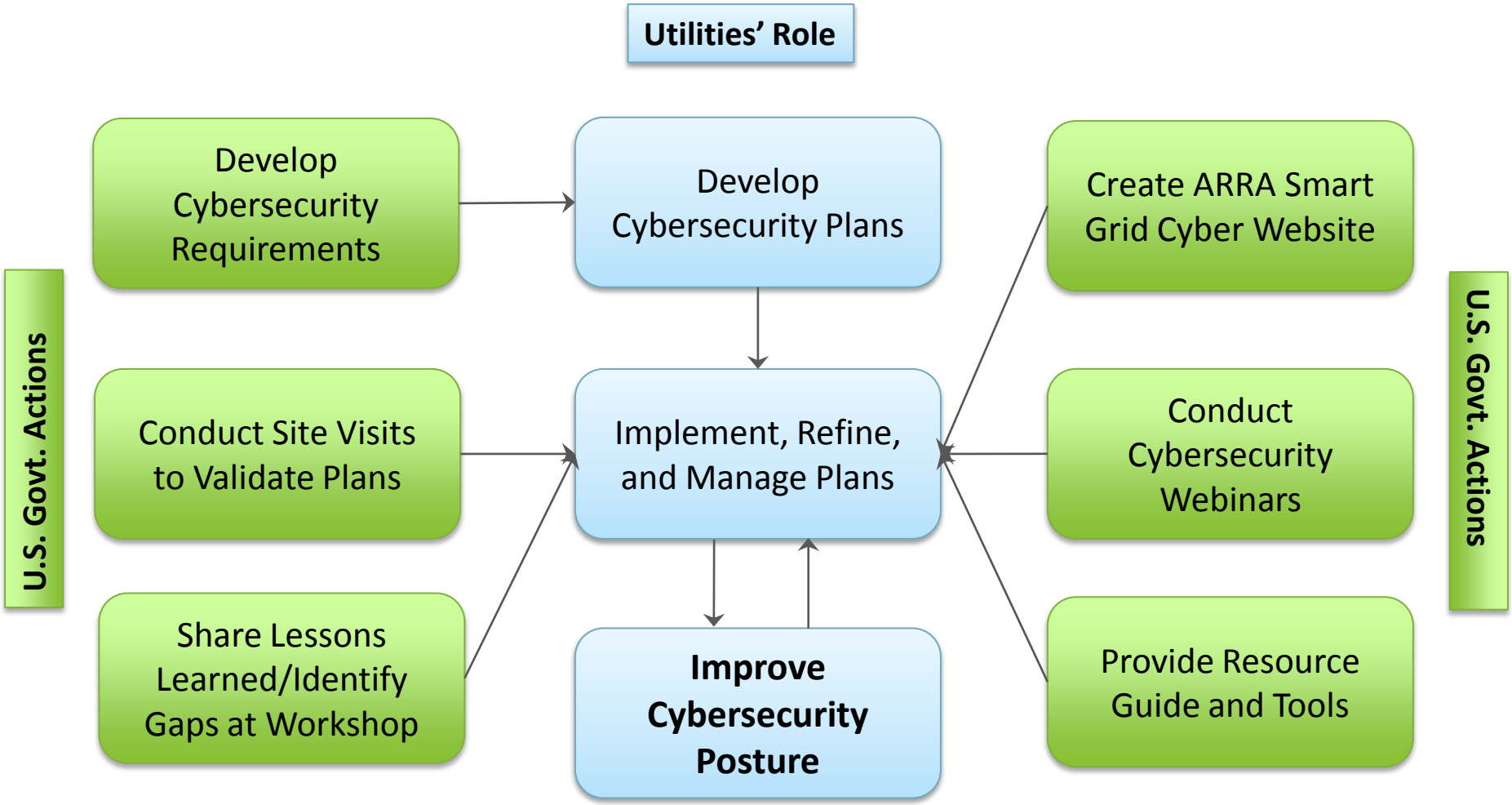
NIST Guidelines for Smart Grid Cybersecurity



- **Supports the design, development, and implementation of cybersecurity measures for smart grid technologies:**
  - Defining the smart grid architecture and high-level security requirements
  - Guiding users to specific existing standards and best practices to secure smart grid architecture components
- **Does NOT prescribe particular solutions, but provides a guideline to evaluate the overall cyber risks to a smart grid system**

19

DOE Cybersecurity Strategy for Smart Grid Investment Grants



SGIG Cybersecurity Milestones

- 99 Cybersecurity Plans developed and approved by DOE
- Nearly 100 site visits completed in 2011; 102 site visits completed in 2012
- 2 Smart Grid Cybersecurity Information Exchanges held: August 2011 and December 2012
- Smart Grid Cybersecurity Resource Tool developed and distributed
- Secure website www.arrasmartgridcyber.net developed for ARRA recipients
- Two cybersecurity webinars conducted by PNNL
- Electricity Subsector Cybersecurity Capability Maturity Model developed and piloted at 17 utilities

Best Practices from Site Visits

Assess, Identify, & Mitigate Risks	• Conduct formal weekly vendor progress reviews • Continue to assess risk throughout all stages of the project's lifecycle
CS Criteria for Vendors & Devices	• Reverse engineer devices and penetration testing to determine security issues • Combine industry screening, bidding to a specification, security questionnaire, & adherence to relevant standards in vendor selection
Adhere to CS Standards & Best Practices	• Project's requirements checklist tool maps every cybersecurity requirement to relevant cyber security standards (e.g., NIST 800-30, ISO 27000, NERC CIP, et al)
Organizational Chain of Accountability	• Executive sponsors and management involved in periodic status meetings, review and approval process and promote/support a strong security culture

Best Practices from Site Visits

CS Risk Assessment Methodology	• Methodology attempts to predict risks prior to exposure and proactively implement mitigating strategies
Assess Impact on Critical Functions	• Weekly meetings ensure that proposed changes to the project do not affect critical grid control functions • Risk-based assessment methodology specified as an annual requirement
Policy, Procedural, & Technical Mitigation	• Major vendor's contract retired to bring key cybersecurity functions back to the enterprise based on unacceptable vendor performance
Confidentiality, Integrity, & Availability	• Strong encryption, VPNs, two-factor authentication, and other best practices to safeguard system data • Strong firewalls, data encryption, intrusion detection, data loss prevention, etc. to include third party communication, and backup off-site

Best Practices from Site Visits

Logging, Monitoring, Alarming, & Notification	• Tamper-alert capabilities on unsupervised field equipment • Firewall, monitoring, and logging from existing security capabilities on internet- facing networks • Logs analyzed daily for anomalies and malware indications; weekly security event reports per established incident response procedure
Logical & Physical Security Not Under Project Jurisdiction	• Remote access by third party to various systems allowed on an as-needed, limited basis and is closely monitored • Project is encrypting data and using VPNs to provide end-to-end security
Updating, Upgrading, & Patching	• Processes support pre-production testing, roll-out into production and reversal if necessary • Strong enterprise update, upgrade, and patch management business process, including testing before deployment • Personnel performance metrics and compensation tied to standards compliance
Test, Demonstrate, Validate, & Document Effectiveness	• Annual internal vulnerability assessments that include both corporate and vendor servers to validate security posture • 3rd-party independent audit conducted to include project's Information Security Program • Internal and external vulnerability assessments of the organization's technical systems

NRECA "Guide to Developing a Cyber Security and Risk Mitigation Plan"

- **What It Is:** An easy-to-navigate guide, risk mitigation checklist, step-by-step template, and 78-question procurement guide
- **How It is Used:** To help electric utilities assess and build an improved cybersecurity plan for their smart grid technologies
- **Created by:** National Rural Electric Cooperative Association (NRECA) with $33.9 million in Recovery Act stimulus funds
- **Who Is Using It:** 23 electric co-ops participating in the NRECA's regional smart grid demonstration project; plus 4,000 downloads from across industry

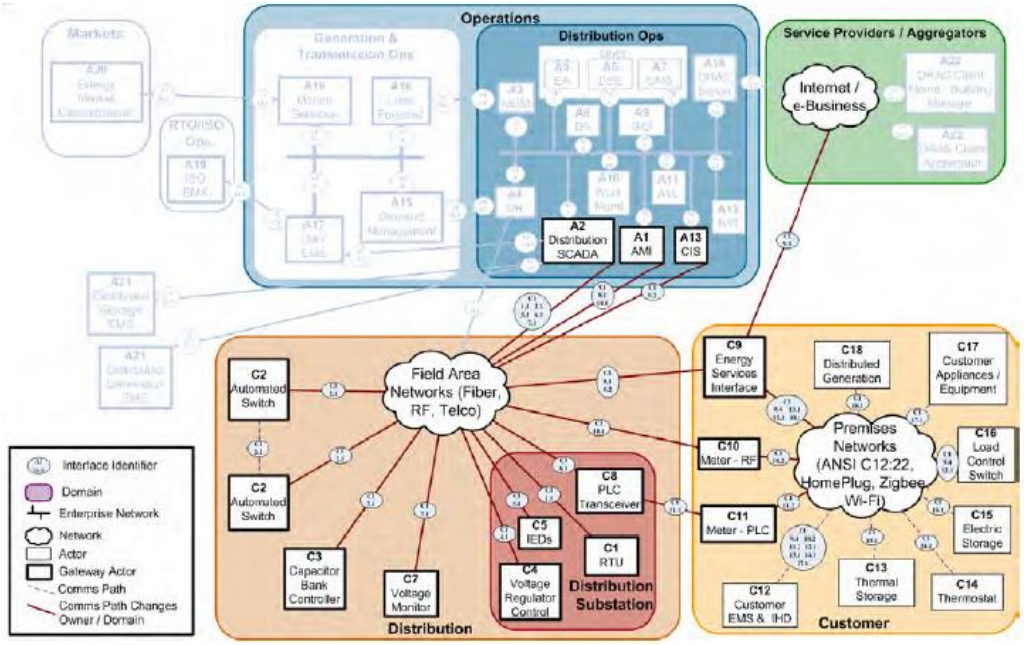
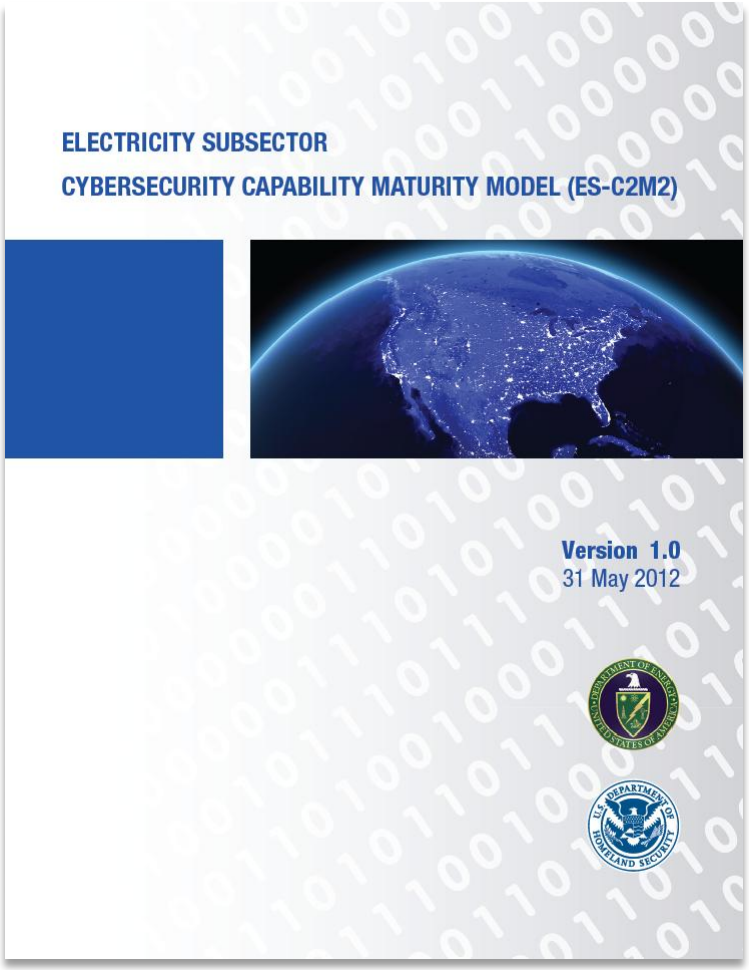


Figure 4. Smart Grid Demonstration Grant Automation Components and Interfaces.

Electricity Subsector Cybersecurity Capability Maturity Model

White House initiative with DHS and industry and cybersecurity experts to develop the **ES-C2M2**, enabling electric utilities and grid operators to:

- Assess their cybersecurity capabilities using a common tool
- Prioritize their actions and investments to improve cybersecurity

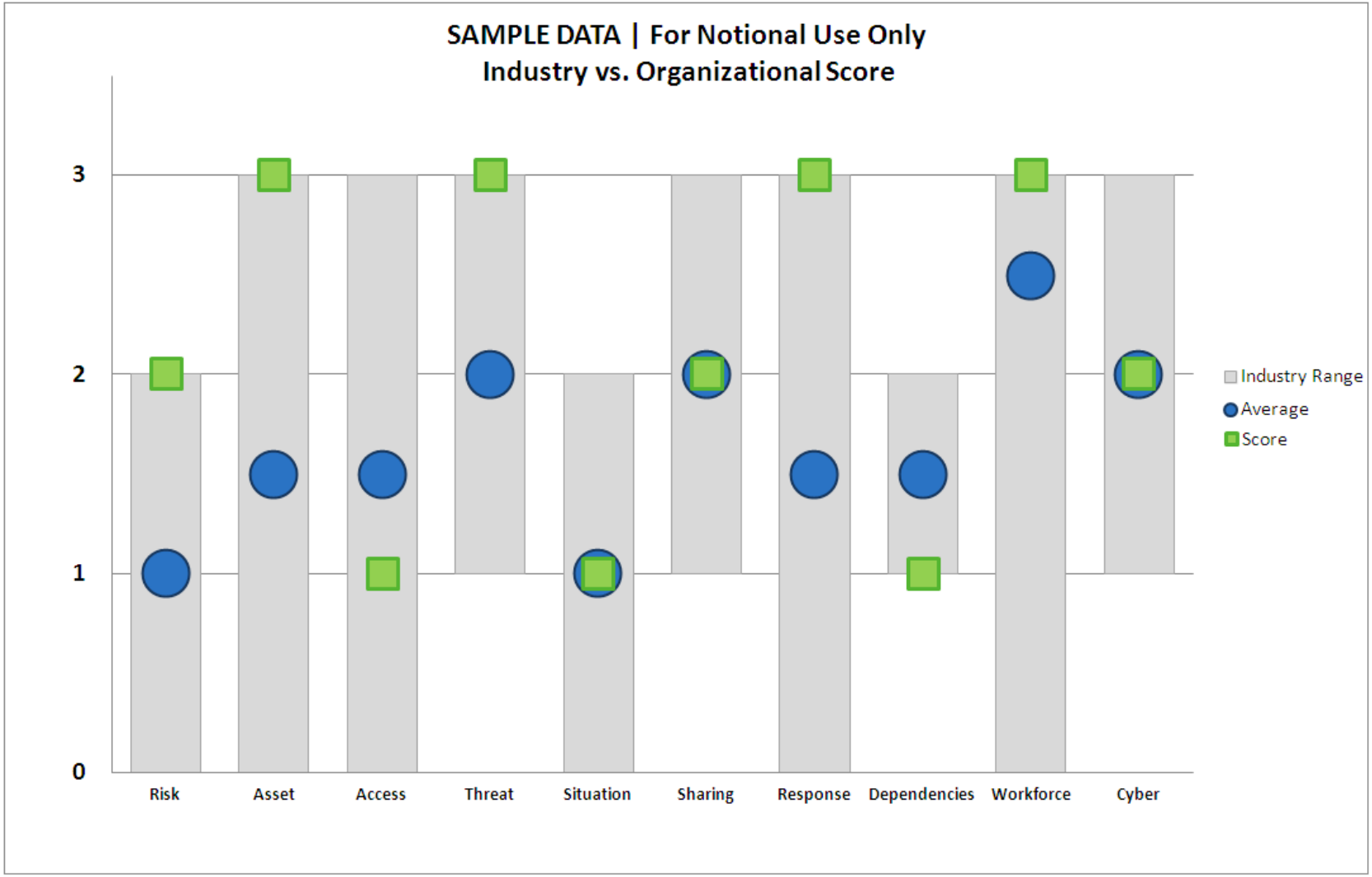


ES-C2M2 Domains

RISK Risk Management	ASSET Asset, Change, and Configuration Management	ACCESS Identity and Access Management	THREAT Threat and Vulnerability Management
SITUATION Situational Awareness	SHARING Information Sharing and Communications	RESPONSE Event and Incident Response, Continuity of Operations	DEPENDENCIES Supply Chain and External Dependencies Management
WORKFORCE Workforce Management	CYBER Cybersecurity Program Management		

- **Domains are logical groupings of cybersecurity practices**
- **Each domain has a short name for easy reference**

Notional Sample Report
Industry Scores vs. Organization



DOE Cybersecurity R&D (CEDS) Aligned with Roadmap

Higher Risk, Longer Term Projects
→ Core NSTB Program
→ Frontier Research
→ Academia Projects
→ Minimum Cost Share

Medium Risk, Mid Term Projects
→ National Laboratory Led Projects
→ Lower Cost Share

Lower Risk, Shorter Term Projects
→ Industry Led Projects
→ Higher Cost Share

Partnering

Path to Commercialization

Core & Frontier (NSTB)
- Argonne National Laboratory
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- Lawrence Berkeley National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratory

Academia – Led
- TCIPG
  - Cornell University
  - Dartmouth College
  - UC-Davis
  - University of Illinois
  - Washington State University
- SEI at Carnegie Mellon

Laboratory – Led
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory

Industry – Led
- Applied Communication Services
- Grid Protection Alliance
- Honeywell
- Schweitzer Engineering Laboratories, Inc.
- Siemens Infrastructure & Cities, Energy Automation
- Sypris

Lemnos Interoperable Configuration Profiles

Products built to a Lemnos configuration profile provide easy interoperability and comparable and compatible cybersecurity functions.

Project Partners:

EnerNex Corporation

TVA

Sandia National Laboratories

SEL Schweitzer Engineering Laboratories

Vendors Using Lemnos:

Industrial Defender

Cisco

n-dimension solutions

Phoenix Contact

Siemens

encore networks

RuggedCom

GarrettCom A Belden Brand

Function/Service	Productivity Benefit
Interoperable configuration of products from different vendors	**Reduced procurement burden and integration costs**
Secure routable data communications between different networks	**Improved control system interconnection and operator efficiency**
Secure remote access from central command	**Cost savings from reduced site visits**
Central access control administration	**Cost savings for administrators**
Central log collection from multiple devices	**Eases NERC CIP compliance**

Padlock Security Gateway

Padlock securely connects distribution field components – low power, low cost gateway with strong access control and password management

Function/Service	Productivity Benefit
Built to Lemnos configuration profiles	**Inherits all Lemnos productivity benefits**
Communication product with integrated security	**Easier patching and reduced engineering and safety costs**
Sensing and notification of physical tampering (coming in 2013)	**Enables automatic quarantine of remote devices**

Project Successes:

- Accelerated commercial release to meet customer demand
- Product shipping daily

Partners: Schweitzer Engineering Laboratories (SEL), Sandia National Laboratories (SNL), Tennessee Valley Authority (TVA)

Network Access Policy Tool (NetAPT) and Sophia Tool

NetAPT generates a network topology description to identify vulnerabilities in a utility's global access policy and allows operators to validate security configurations

Project Successes:

- Developed by TCIPG.
- More than 20 copies of NetAPT have been licensed; DHS funding commercialization
- TCIPG's industry partners are now using NetAPT for vulnerability assessments and compliance audits
- **Sophia** was beta tested by 29 industry participants and is moving toward commercialization

Function/Service	Productivity Benefit
Rapid identification of cyber assets from automated network topology development	**NERC CIP audit time requirement reduced from weeks to minutes**
Easy network topology updates following firewall configuration changes	**Removal of manual adjustments to adjust the network topology**
Sophia allows fast alerting of unexpected communication access or traffic	**Attack interruption and minimized consequences of attack**

Visit:

SMARTGRID.GOV

for more information