NIST Smart Grid Program

Interoperability and Cybersecurity in the Smart Grid

George Arnold, Eng.Sc.D.

National Coordinator for Smart Grid Interoperability

National Institute of Standards and Technology

TCIPG Seminar Series on Technologies for a Resilient Power Grid

University of Illinois

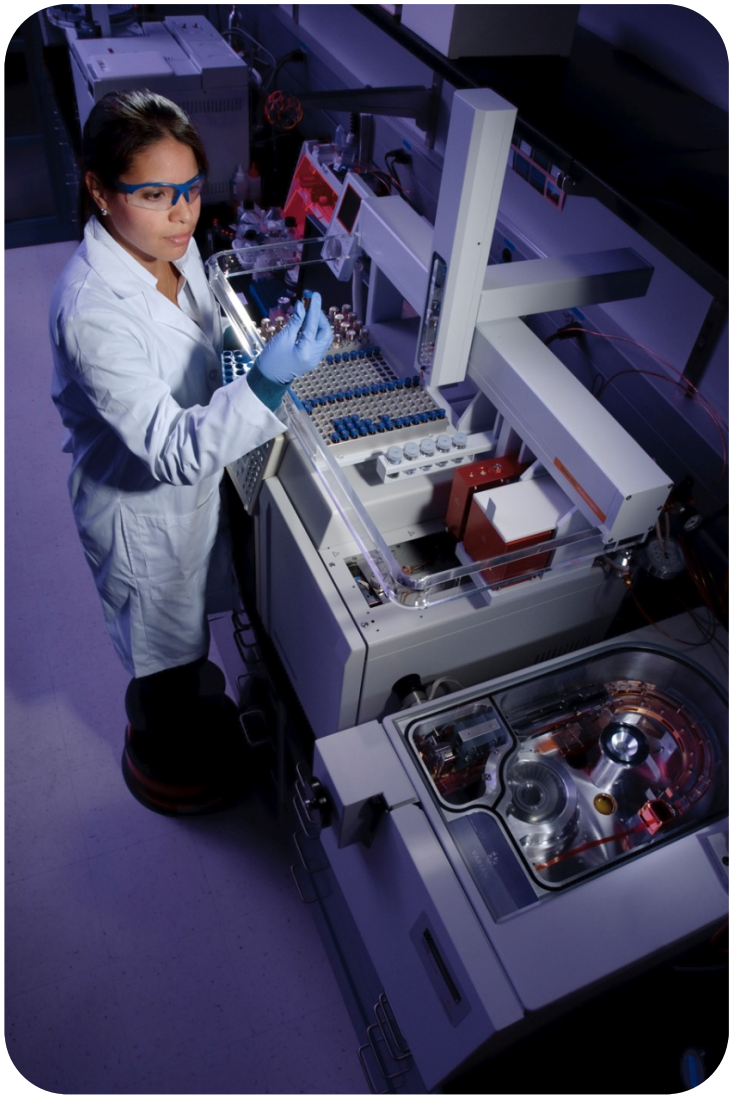
February 1, 2013

NIST National Institute of Standards and Technology U.S. Department of Commerce

engineering laboratory

NIST's Mission

To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life.



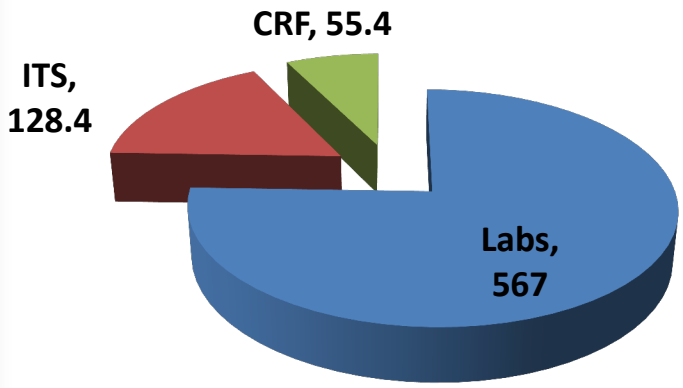
©R. Rathe

NIST: Basic Stats and Facts

Major assets

- ~ 3,000 employees
- ~ 2,800 associates and facilities users
- ~ 1,600 field staff in partner organizations (Manufacturing Extension Partnership)
- Two locations: Gaithersburg, Md., and Boulder, Colo.
- Four external collaborative institutes: basic physics, biotech, quantum, and marine science

FY 2012 Appropriations $750.8 M



NIST Priority Research Areas


TebNad

Energy


S.Bonk

Environment


Fotocrisis

Manufacturing


Y. Arcurs

Healthcare


designersart

Information Technology and Cybersecurity

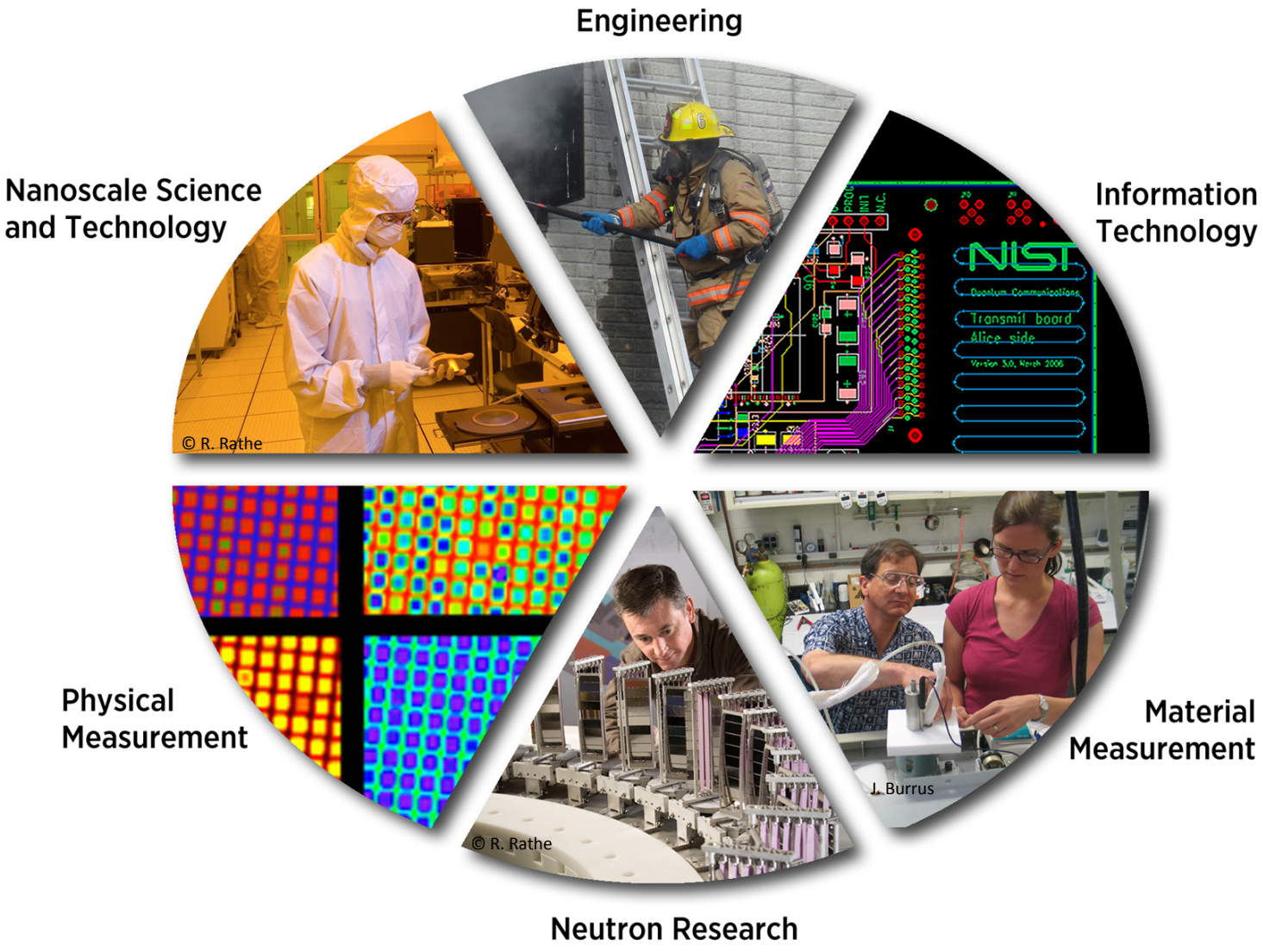

Jovan Nikolic

Physical Infrastructure


Chuck Rausin/shutterstock.com

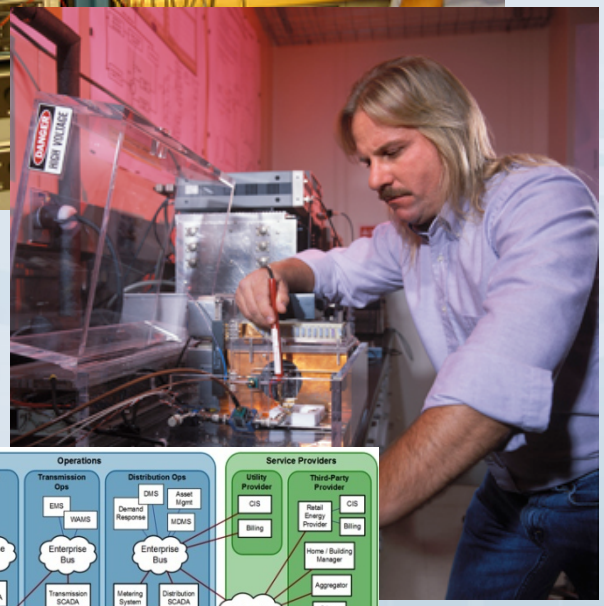
All photos courtesy Shutterstock.com

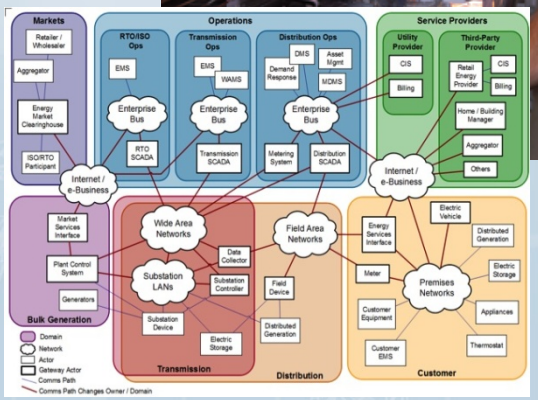
NIST Laboratories



NIST Roles in the Smart Grid

- Measurement research
  - Metering
  - Wide area situational awareness (PMUs)
  - Power electronics
  - Network communications
  - Timing
  - Building energy management
  - Others …
- Standards
  - Interoperability
  - Cybersecurity

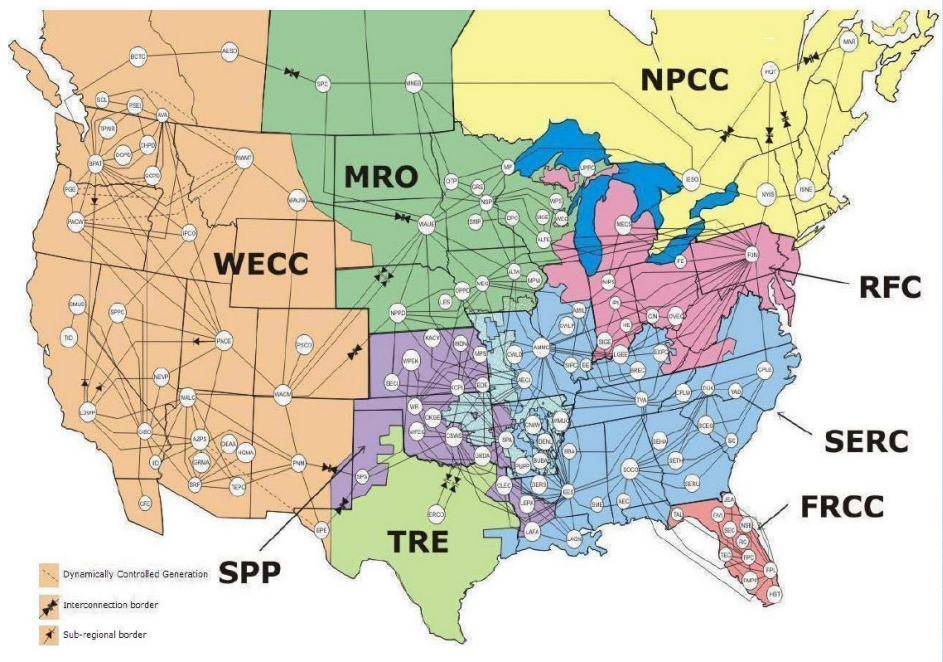




U.S. Electric Grid: A Large, Fragmented, Complex System

US figures:

- 22% of world consumption



- 3,200 electric utility companies
- 17,000 power plants
- 800 gigawatt peak demand
- 165,000 miles of high-voltage lines
- 6 million miles of distribution lines
- 140 million meters
- $1 trillion in assets
- $350 billion annual revenues

Drivers for Grid Modernization

Greater efficiency to reduce need for asset replacement and system expansion: $1.5-$2 trillion by 2030

Increased reliability: power outages cost the US economy $80 billion/year

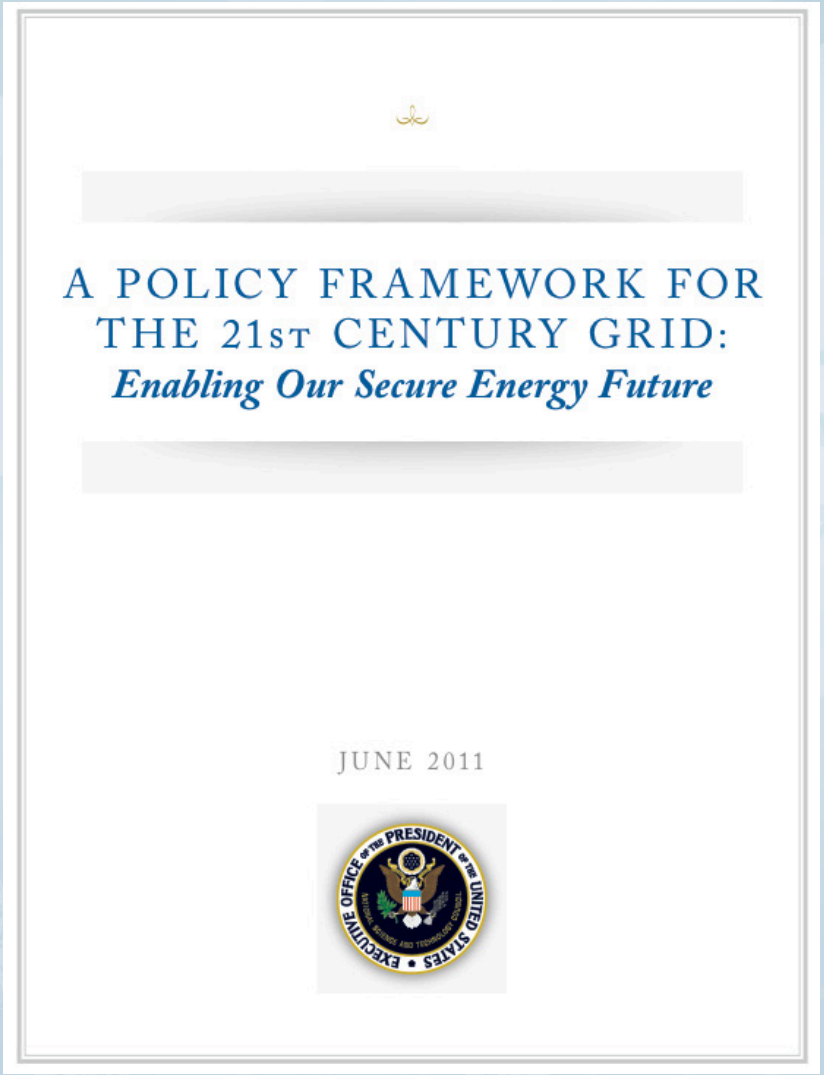
Sustainability: 29 states have renewable portfolio standards

2011 EPRI study:
Smart Grid will cost in the range of $338 - $476 billion over 20 years
Resulting benefit estimated at $1.6 - $2 trillion

Smart Grid – A U.S. National Policy

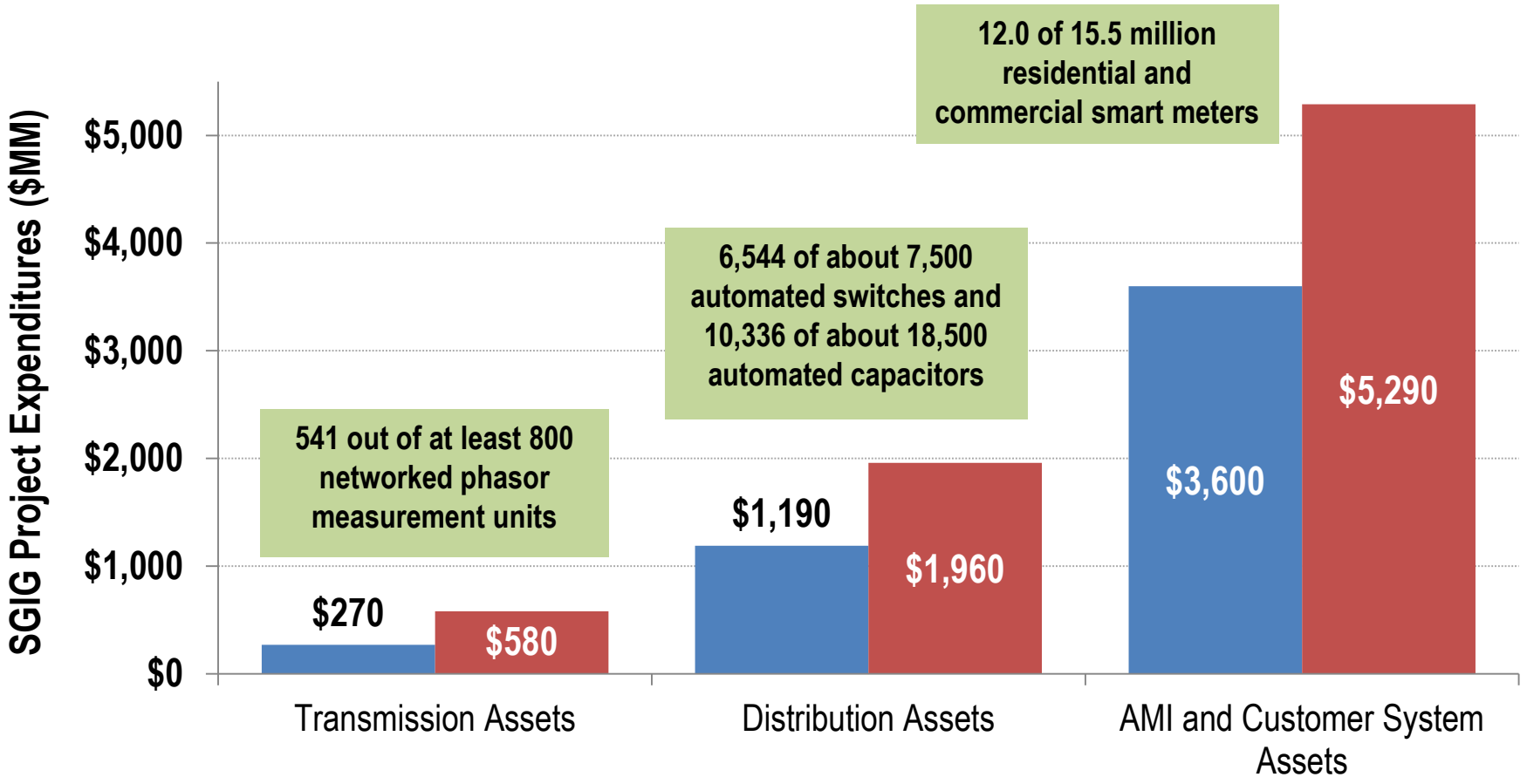
- "It is the policy of the United States to support the modernization of the Nation's electricity [system]… to achieve…a Smart Grid."

- *Congress, Energy Independence and Security Act of 2007*



http://www.whitehouse.gov/ostp

SGIG Deployment Status



* Based on self-reported project target from Recipients.

Peak and Overall Demand Reduction via AMI, Pricing and Customer Systems

62 SGIG projects (pricing and customer systems offered mostly at pilot scales):

- **56 offering web portals; 46 offering (DLC, PCTs, and/or IHDs)**
- **32 offering pricing (TOU, CPP, CPR, VPP)**

Project Elements	OG&E 770,000 customers	MMLD 11,000 customers	SVE 18,000 customers
Customers Tested	6,000 residential	500 residential	600 mostly residential
Time-Based Rate(s)	TOU and VPP, w/CPP	CPP	CPP
Customer Systems	IHDs, PCTs, and Web Portals	Web Portals	Web Portals
Peak Demand Reduction	Up to 30% 1.3 kW/customer (1.8 kW/customer w/CPP)	37% 0.74 kW/customer	Up to 25% 0.85 kW/customer
Outcome	Deferral of 210 MW of peak demand by 2014 with 20% participation	Lowers total purchase of peak electricity	Lowers total purchase of peak electricity
Customer Acceptance	Positive experience, many reduced electricity bills	Positive experience, but did not use the web portals often	Interested in continued participation, many reduced electricity bills

Reliability Improvements

48 SGIG projects are applying distribution automation technologies to improve reliability:

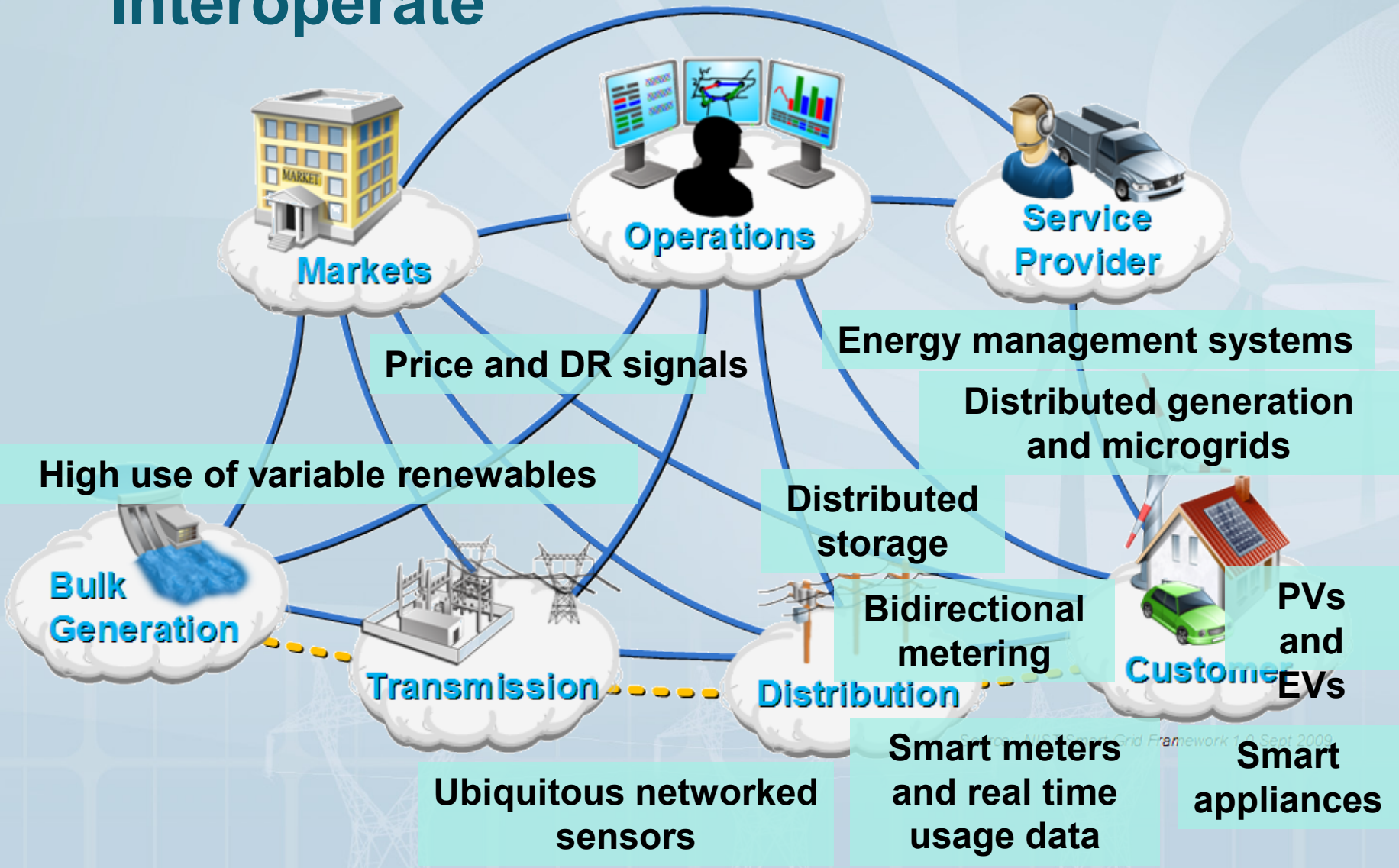
- **42 deploying automated feeder switches (1 to > 1000's of switches)**
  - **Enables fault location, isolation and service restoration functions (FLISR)**
- **Multitude of system integration schemes (AMI/OMS/DMS/SCADA/GIS)**
  - **26 projects are applying distribution management systems**
  - **36 implementing AMI outage notification**
  - **22 deploying equipment health sensors**

Initial results from 4 Projects (1,250 feeders) – April 1, 2011 through March 31, 2012

Reliability Index	Description	Weighted Average (Range)
SAIFI	**System Average Interruption Frequency Index (outages)**	**-22 %** (-11% to -49%)
MAIFI	**Momentary Average Interruption Frequency Index (interruptions)**	**-22 %** (-13% to -35%)
SAIDI	**System Average Interruption Duration Index (minutes)**	**-18 %** (+4% to -56%)
CAIDI	**Customer Average Interruption Duration Index (minutes)**	**+8 %** (+29% to -15%)

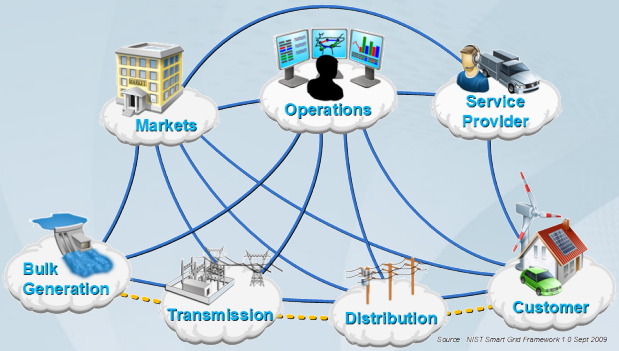
Weighted average based on numbers of feeders

Many Devices and Systems Need to Interoperate



Ubiquitous Networked Sensors

Paradigm Shift → Smart Grid



From:

- Vertically integrated monopolies
- Centralized fossil fuel generation
- Limited awareness
- Hierarchical network
- Deterministic control
- Generation to meet demand
- Proprietary architectures and interfaces

To:

- Restructured competitive markets
- More distributed and renewable generation
- Sensors everywhere
- Interconnected microgrids
- Stochastic control
- Responsive demand and generation
- Open standards

Standards for the Grid in U.S. Law

The Energy Independence and Security Act directs NIST

"to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"

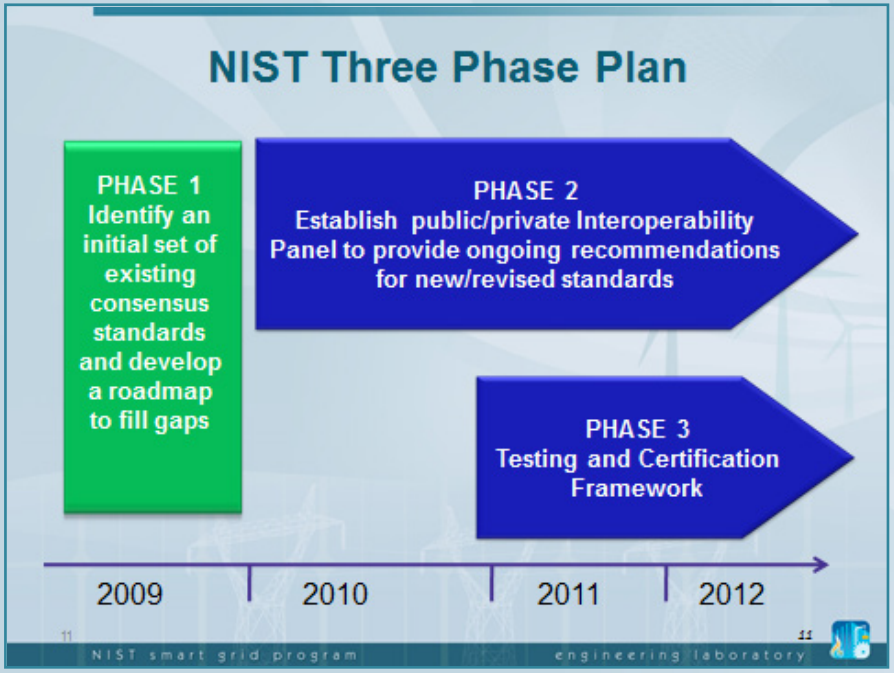
- Congress directed that the framework be "flexible, uniform, and technology neutral"
- Use of these standards is a criteria for Dept. of Energy Smart Grid Investment Grants
- Input to federal and state regulators

Standards Come From Many Sources

Stakeholders in the Process

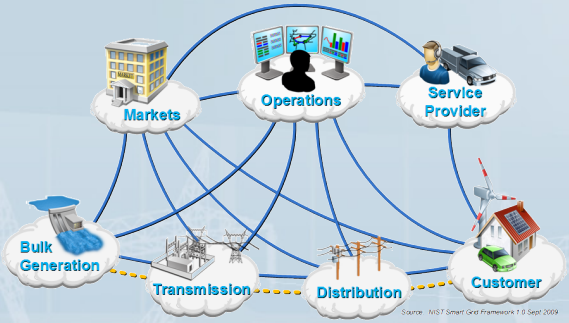
1	Appliance and consumer electronics providers
2	Commercial and industrial equipment manufacturers and automation vendors
3	Consumers – Residential, commercial, and industrial
4	Electric transportation industry Stakeholders
5	Electric utility companies – Investor Owned Utilities (IOU)
6	Electric utility companies - Municipal (MUNI)
7	Electric utility companies - Rural Electric Association (REA)
8	Electricity and financial market traders (includes aggregators)
9	Independent power producers
10	Information and communication technologies (ICT) Infrastructure and Service Providers
11	Information technology (IT) application developers and integrators
12	Power equipment manufacturers and vendors
13	Professional societies, users groups, and industry consortia
14	R&D organizations and academia
15	Relevant Government Agencies
16	Renewable Power Producers
17	Retail Service Providers
18	Standard and specification development organizations (SDOs)
19	State and local regulators
20	Testing and Certification Vendors
21	Transmission Operators and Independent System Operators
22	Venture Capital

NIST Plan – and – NIST Framework 2.0

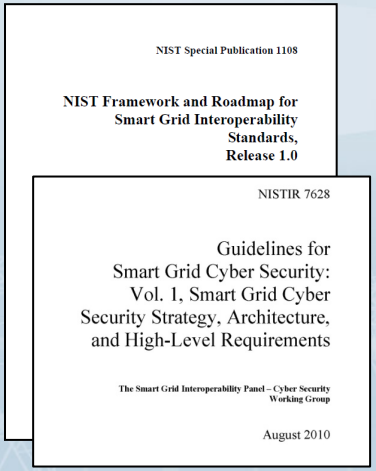


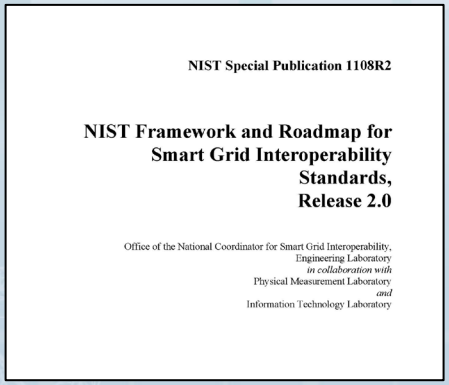
- Release 2 - February 2012
- Release 1 - January 2010
- Smart Grid vision & reference model
- Identifies 100 standards
- Cybersecurity guidelines
- Testing and certification framework
- Provided a foundation for IEC, IEEE, ITU, and other national and regional standardization efforts

White House kickoff and NIST stakeholder meetings



NIST Smart Grid Domains



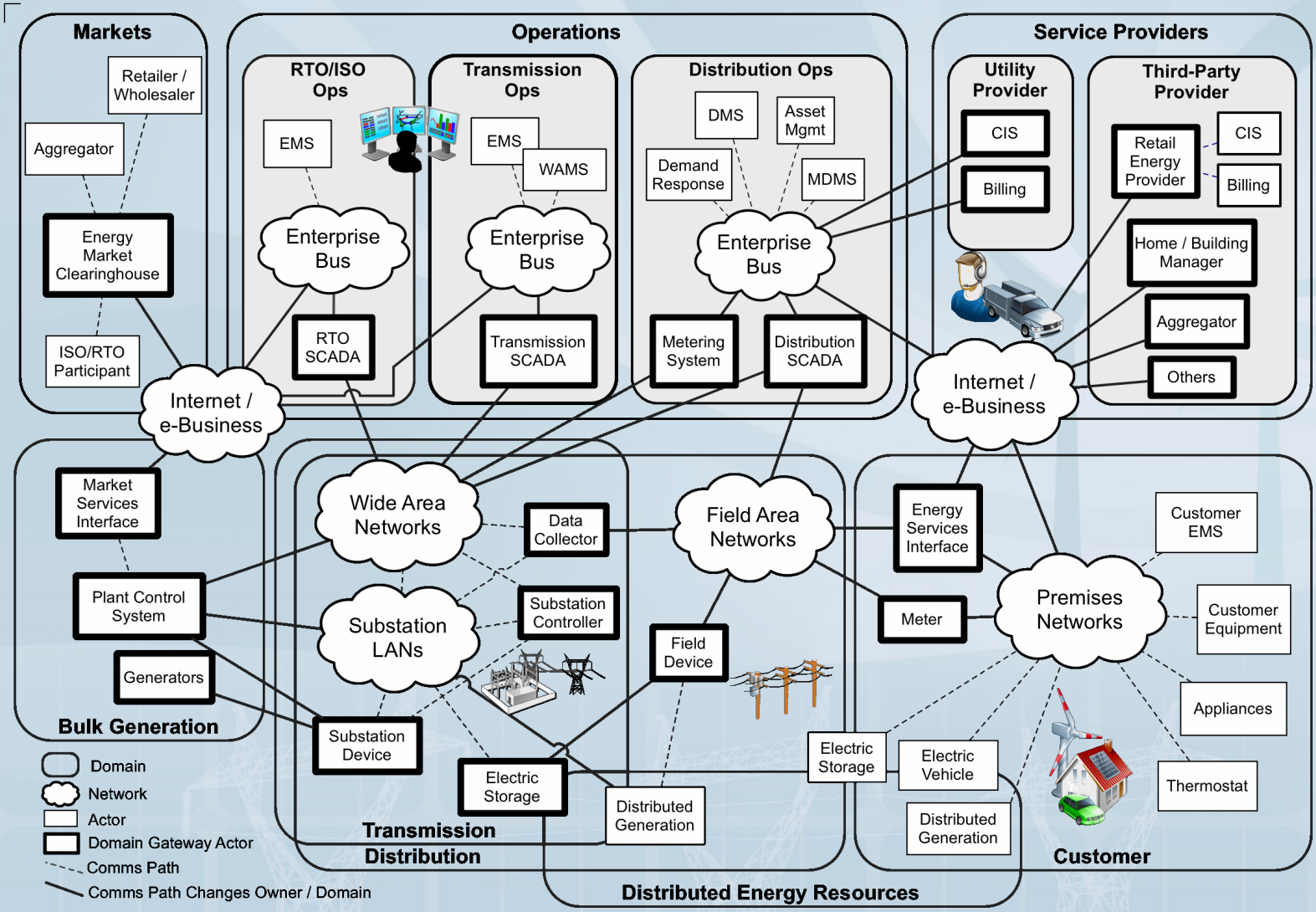


http://www.nist.gov/smartgrid/

Priority Use Cases for Standardization

- Demand Response and Consumer Energy Efficiency
- Wide Area Situational Awareness
- Electric Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management
- Cyber Security
- Network Communications

NIST Smart Grid Reference Model (Release 2.0)



Smart Grid Interoperability Panel

- Public-private partnership created in Nov. 2009
- 780+ member organizations, 1,900+ individual participants
- Open, public process with international participation
- Web-based participation
- Coordinates standards developed by Standards Development Organizations (SDOs)
  - Identifies requirements and prioritizes standards development programs
  - Works with over 20 SDOs including IEC, ISO, ITU, IEEE, …
  - IEC, IEEE and ITU roadmaps are all based on the NIST/SGIP Framework
- New SGIP 2.0 legal entity established



SGIP
SMART GRID INTEROPERABILITY PANEL

Standing Committees

- Architecture (SGAC)
  - Responsible for creating and refining an architectural reference model, including recommended standards and profiles necessary to implement the vision of the Smart Grid.
  - Chair: Ron Ambrosio, IBM
- Testing & Certification (SGTCC)
  - Responsible for creating and maintaining the necessary documentation and organizational framework for testing conformance with these Smart Grid standards and specifications.
  - Chair: Rik Drummond, Drummond Group

Standing Committees

- Implementation Methods Committee (SGIMC)
  - Identify, develop and support mechanisms and tools for objective standards impact assessment, transition management and technology transfer in order to assist in deployment of standards based Smart Grid devices, systems and infrastructure.
  - Co-Chairs: Bill Cloutier, DTE Energy and Christine Wright, Public Utilities Commission of Texas

Standing Committees

- Cybersecurity Committee (SGCC)
  - Develop an overall cyber security strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure.
  - Chair: Marianne Swanson, NIST

Domain Expert Working Groups (DEWGS)

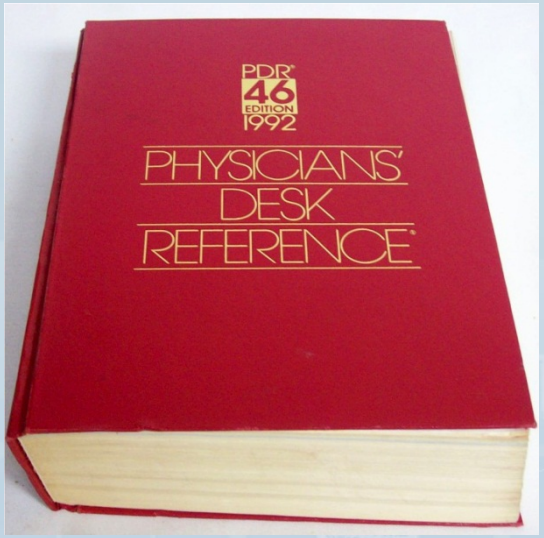
- Home-to-Grid (H2G)
  - Applications and communications linking energy service providers (utilities and othefr third-party providers) with customer equipment in residential buildings via the electric grid and associated networks
- Building-to-Grid (B2G)
  - Commercial building interaction with the electric grid, including the energy service provider as well as other grid-side service partners
- Industry-to-Grid (I2G)
  - Interoperability and interaction between the electric grid and industrial facilities, including electric power generation
- Vehicle-to-Grid (V2G)
  - Plug-in electric vehicle (PEV) interaction with the electric grid, including discharging as well as charging and customer-utility interactions

DEWGS (cont)

- Transmission and Distribution (TnD)
  - Utility transmission and distribution operations as well as interactions with other producer/users on the grid
- Business and Policy (BnP)
  - Assist business decision-makers and legislative/regulatory policy-makers in implementing smart grid policies sensitive to interoperability
- Distributed Renewables, Generators and Storage (DRGS)
  - Identify and define standards and interoperability issues and gaps related to Smart Grid integration of distributed renewable/clean energy generators and electric storage and to initiate priority action plans and task groups to address these issues and gaps
- Electromagnetic Interference Issues Working Group (EMIIWG)
  - will investigate enhancing the immunity of Smart Grid devices and systems to the detrimental effects of natural and man-made electromagnetic interference, both radiated and conducted.

SGIP Catalog of Standards

- The analog of the "Physician's Desk Reference" for the Smart Grid



ID	Attribute	Standard Information
	Section I: Use and Application of the Standard	
A	Identification and Affiliation	
1	Identifier of the standard	REQ 18, WEQ19
2	Title of the standard	NAESB PAP10 Energy Usage Information
3	Name of owner organization	NAESB
4	Latest versions, stages, dates	Revision 1.0 December 2010
5	URL(s) for the standard	http://www.naesb.org/member_login_check.asp?doc=weq_rat102910_weq_2010_ap_6d_rec.doc , http://www.naesb.org/member_login_check.asp?doc=req_rat102910_req_2010_ap_9d_rec.doc
6	SSO Working Group / Committee responsible for the standard	REQ, WEQ
7	Original source of the content (if applicable)	
8	Brief description of scope	Customers will benefit from energy usage information that enables them to make better decisions and take other actions consistent with the goals of Sections 1301 and 1305 of EISA. An understanding of energy usage informs better decisions about energy use and conservation, and is the basis for performance feedback on the operation of customer-owned energy management systems and understanding device energy usage and management. This standard defines an information model of semantics for the definition and exchange of customer energy usage information. The actual exchange standards are anticipated to be derivative from this seed standard.
B	Level of Standardization	
1	Names of standards development organizations that recognize this standard and/or accredit the owner organization	ANSI
2	Has this standard been adopted in regulation or legislation, or is it under consideration for adoption?	No
3	Has it been endorsed or recommended by any level of government? If "Yes", please describe	No
4	Level of Standard (check all that apply)	☐ International ☑ National ☐ Regional ☐ deFacto ☐ Single Company
5	Type of document	Standard
6	Level of Release	Released
C	Conceptual Model Areas of Use	
1	Currently applies to which domains? (check all that apply)	☑ Market ☑ Operations ☑ Service Provider ☑ Generation ☐ Transmission ☐ Distribution ☑ Customer
2	Planned for use in which domains? (check all that apply)	☑ Market ☑ Operations ☑ Service Provider ☐ Generation ☐ Transmission ☐ Distribution ☑ Customer

SGIP Catalog of Standards

Criteria for inclusion

- Formalized SGIP process for evaluation and decision to include
- Requires reviews by architecture, cybersecurity, and domain expert committees
- Criteria
  - Relevant to advancing interoperability of Smart Grid devices and systems
  - Accepted by the community
  - Suitable for deployment
  - Focuses on interfaces to facilitate integration and promote implementation flexibility
  - Documented and maintained by multi-member organization

Information included in catalog for each standard

- Development organization and process
- Support, conformance, certification, and testing
- Application domains targeted by the standard
- Interoperability categories covered by the standard (organizational, informational, technical layers)
- Cybersecurity and privacy aspects
- Recommendations resulting from reviews

Example: Green Button

- *Enables electricity customers to access their own energy usage information in a consumer- and computer-friendly electronic format from their utility's secure website*
- *Result of collaboration among White House, DOE, NIST, state regulators, utilities, vendors, SGIP, and North American Energy Standards Board*

15+ million consumers have access to Green Button data NOW, and 36+ million will by 2013

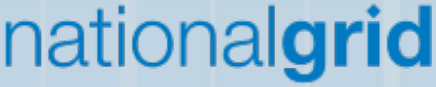
Green Button
Download
My Data

www.greenbuttondata.org & www.nist.gov/smartgrid/greenbutton.cfm

Source:

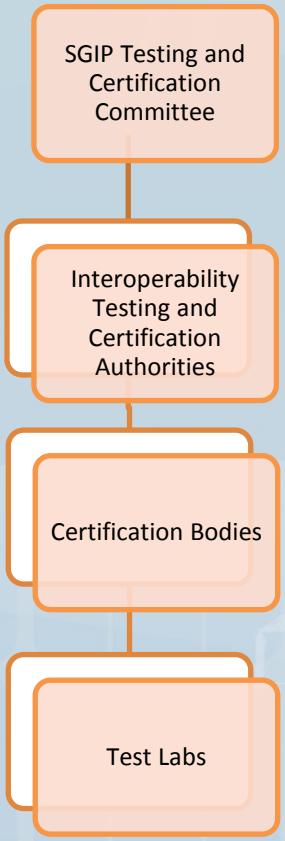
The ecosystem of companies and organizations supporting and using Green Button data…

- Utilities
- Utility software vendors
- Apps developers
- Device manufacturers
- Standards organizations



Testing and Certification Framework

- Defined in SGIP Interoperability Process Reference Manual (IPRM)



SGIP IPRM documents requirements and best practices for ITCAs, CBs and TLs

ITCAs establish T&C schemes for specific domains/use cases and accredit CBs and TLs
Initially-identified ITCAs: NEMA, UCAIug 61850, OpenADR, and Multispeak, SEP 2.0

Certify test results

Perform conformance and/or interoperability testing to specified test cases


SMART GRID INTEROPERABILITY PANEL

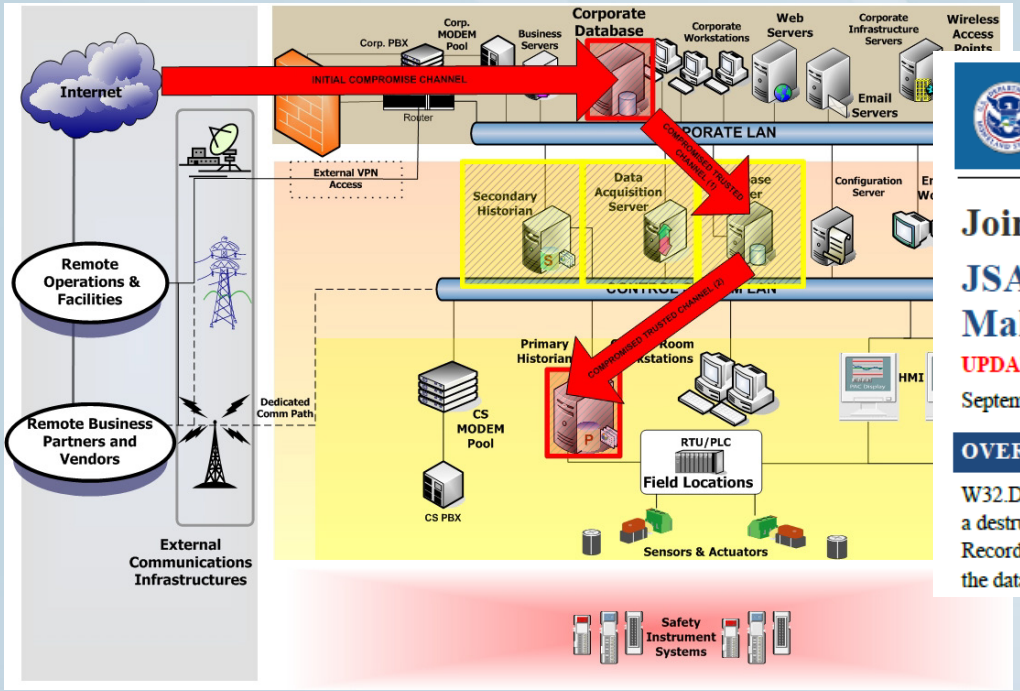
Smart Grid Testing & Certification Committee (SGTCC)

Interoperability Process Reference Manual (IPRM)

Version 2.0

January 2012

Interconnected Networks and Intelligence Create New Vulnerabilities



ICS-CERT
Industrial Control Systems Cyber Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Joint Security Awareness Report

JSAR-12-241-01A—Shamoon/DistTrack Malware

UPDATE A

September 27, 2012

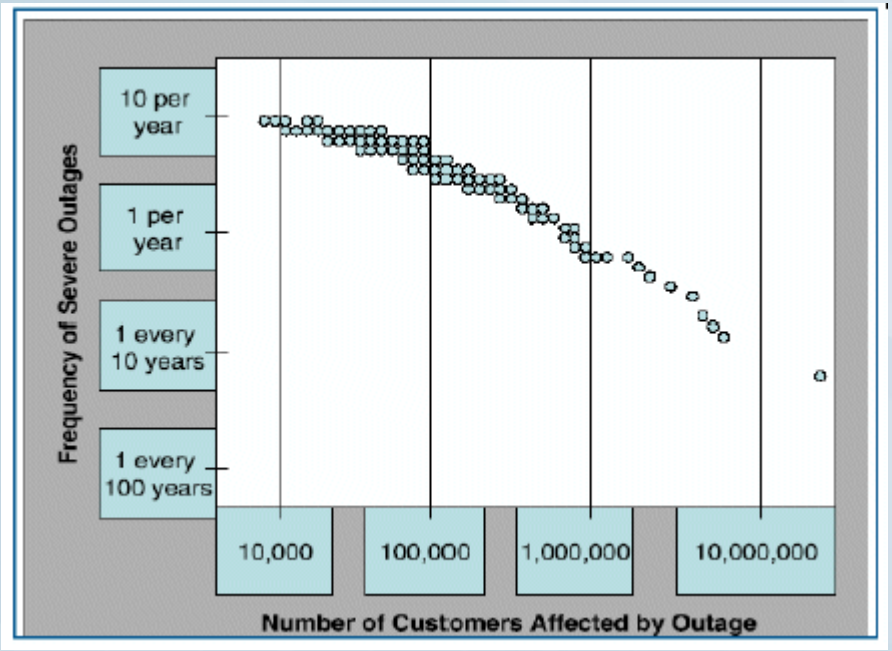
OVERVIEW

W32.DistTrack, also known as "Shamoon," is an information-stealing malware that also includes a destructive module. Shamoon renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

"An unauthenticated attacker with network access to the CK721-A device can instruct it to perform various tasks like unlocking a door, adding badges, or changing the configuration which could grant physical access to a secured area. "

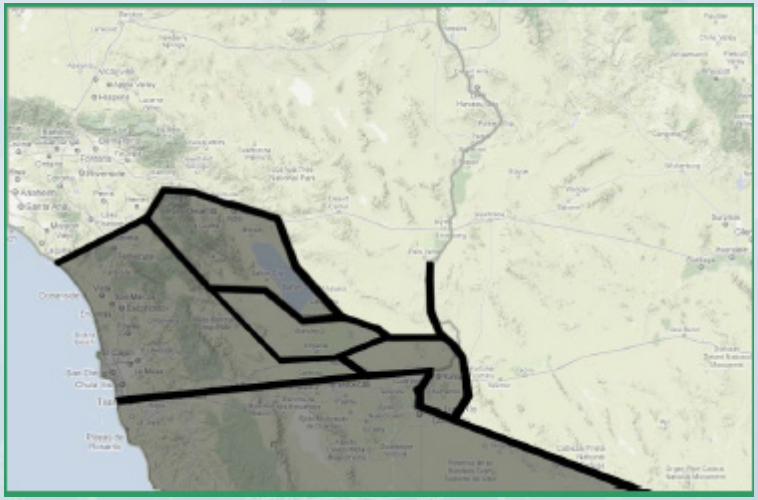
Failures Can Cascade Quickly in Today's Power Grid

North American Power System Outages



Note: The circles represent individual outages in North America between 1984 and 1997, plotted against the frequency of outages of equal or greater size over that period.
Source: Adapted from John Doyle, California Institute of Technology, "Complexity and Robustness," 1999. Data from NERC.

San Diego (2011): 7 million people lost power in 11 minutes



Source: FERC/NERC Staff Report on Arizona – Southern California Outages on Sept. 8, 2011

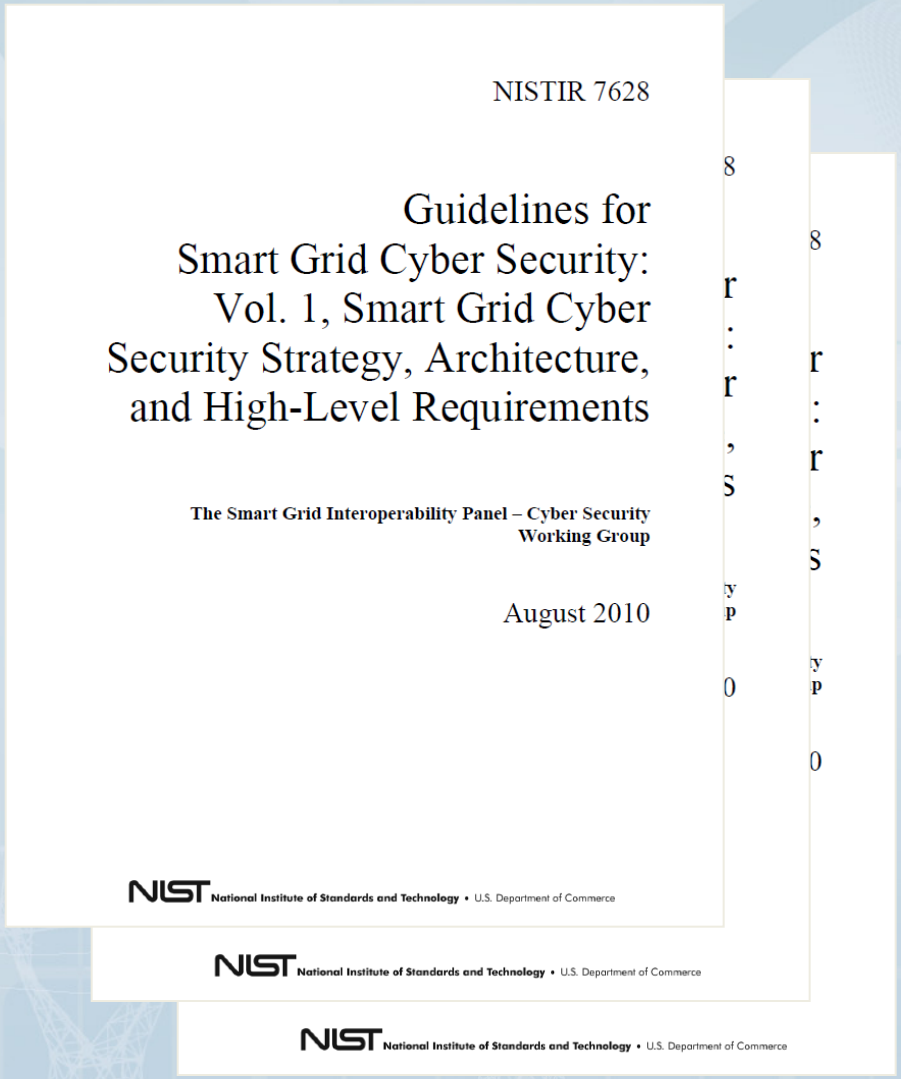
The Cybersecurity Committee Management Team

- Marianne Swanson – NIST Chair
- Akhlesh Kaushiva – Department of Energy, Vice Chair
- Scott Saunders – Sacramento Municipal Utility District, Vice Chair
- Dave Dalva – Stroz Friedberg, Vice Chair
- Mark Enstrom – NeuStar, Secretary
- Tanya Brewer – NIST
- Victoria Yan Pillitteri – NIST

Guidelines for Smart Grid Cyber Security

NIST Interagency Report 7628 - August 2010

- Development of the document lead by NIST
- Represents significant coordination among
  - Federal agencies
  - Private sector
  - Regulators
  - Academics



NISTIR 7628 Provides

- An overview of the Smart Grid cybersecurity strategy and high- level cybersecurity requirements;
- A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies—established and emerging;
- An evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation, and maintenance; and
- A guide to assist organizations as they craft a Smart Grid cybersecurity strategy that includes requirements to mitigate risks and privacy issues pertaining to Smart Grid customers and uses of their data.

NISTIR 7628 Is NOT

- A prescription for particular situations and solutions
- A set of mandatory requirements

- Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.
- NISTIR 7628 provides or has references to methodology, tools and best practices to help organizations develop their cybersecurity strategy and risk assessment

NISTIR 7628 Contents

- Introduction http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf
- Volume 1 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
- Volume 2 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf
- Volume 3 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

- Executive summary of the Guidelines
- Strategy, architecture, high-level security requirements, mapping of security standards documents (NIST 800-53, DHS Catalog, and NERC CIPs) and available technologies to requirements
- Privacy
- Supportive analyses and references – includes extensive identification of vulnerabilities and use cases

Cybersecurity Committee Active Sub-groups and Leads

- **Architecture Group**
  - Elizabeth Sisley
- **Cloud Computing and Smart Grid**
  - Marianne Swanson
- **High-Level Requirements Group**
  - Dave Dalva & Victoria Yan Pillitteri
- **NISTIR 7628 Users Guide Group**
  - Chris Rosen & Mark Ellison
- **Privacy Group**
  - Rebecca Herold
- **Standards Group**
  - Frances Cleveland

R&D Priorities: Cyber-Physical Vulnerabilities and Threats

- Detecting anomalous behavior using modeling
- False data injection – detection and mitigation
- Cost-effective tamper-resistant devices (sensors and actuators)
- Intrusion detection in embedded processors
- Key management and cryptography for embedded devices – lightweight, low power
- System-level architecture for bounded reaction and recovery
- Legacy system integration

Learning More and Getting Involved

- Learn more about the SGCC at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
- Learn more about the subgroups, including meeting times: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo
- To learn more about SGIP 2.0 and join, visit: http://sgip.org/
- Download NISTIR 7628 at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
- For any questions or comments, please contact Marianne Swanson, SGCC Chair, at marianne.swanson@nist.gov

Further Information and Assistance

- Web portal: http://www.nist.gov/smartgrid
- Contact:
  - George Arnold, National Coordinator
  - Email: george.arnold@nist.gov
  - Telephone: +1.301.975.2232