Smart Grid and Cyber Security for Energy Assurance

Planning Elements for Consideration in States' Energy Assurance Plans

National Association of State Energy Officials

Disclaimer of Warranties and Limitation of Liabilities

Acknowledgment of work by the National Association of State Energy Officials (NASEO) contributing to this effort:

This material is based upon work supported by the Department of Energy under award number DE-OE0000119.

Disclaimer:

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

National Association of State Energy Officials (NASEO)
1414 Prince Street, Suite 200, Alexandria, VA 22314 | Phone: 703.299.8800
Revised: November 2011

Cover Photo courtesy of the Electric Power Research Institute.

Smart Grid and Cyber Security for Energy Assurance

Planning Elements for Consideration in States' Energy Assurance Plans

National Association of State Energy Officials

Acknowledgements

The National Association of State Energy Officials (NASEO) prepared this report to support State efforts to update and revise their State energy assurance plans. NASEO's work on this report was funded by the U.S. Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability (OE). Alice Lippert of DOE/OE has been a key supporter of the effort to assure that smart grid and cyber security are included in State plans.

Jeffrey Pillon, NASEO Director of Energy Assurance, led the development of this report. Additional contributors and reviewers include a number of Electric Power Research Institute (EPRI) staff, particularly Ellen Petrill, and contributions by Erfan Ibrahim, Matt Wakefield, and others; members of EPRI Energy Efficiency/Smart Grid Public Advisory Group; EPRI members on the IntelliGrid Steering Committee and other Power Delivery & Utilization members; Darren Highfill of the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) and the Smart Grid Security Working Group; the NASEO Energy Data and Security Committee; and the National Association of Regulatory Utility Commissioners (NARUC) Critical Infrastructure Committee and Staff Subcommittee. Lisa Carrington, Program Manager, National Electric Sector Cybersecurity Organization (NESCOR) also contributed to an update of that organizations current efforts. NASEO gratefully acknowledges the contributions from these individuals and organizations.

Table of Contents

Smart Grid and Cyber Security for Energy Assurance

Planning Elements for Consideration in States' Energy Assurance Plans

Section 1 – Introduction

Energy assurance—a major element of improving the nation's energy sector resiliency—involves a broad range of activities within three main phases: preparation and planning, mitigation and response, and education and outreach.

- *Preparation and planning* involve identifying key assets and points-of-contact, designing and updating energy assurance and emergency response plans, training personnel, and conducting exercises that test the effectiveness of response plans.
- *Mitigation and response* activities include monitoring events that may affect energy supplies, assessing the severity of disruptions, providing situational awareness, coordinating restoration efforts, and tracking recoveries.
- *Education and outreach* activities include communicating and coordinating with key stakeholders, increasing public awareness, and forming partnerships across sectors and jurisdictions.[1]

As grid modernization evolves, smart grid and cyber security factors have emerged as critical factors in energy assurance planning. A "smarter" grid and its related components allow for more timely and accurate power outage information, better self-healing capabilities and outage prevention, and enhanced demand response and renewables integration. Altogether the smart grid is intended to reduce electricity system vulnerabilities and risks and improve emergency response. Cyber security becomes a greater concern with an increasingly complex grid that is more reliant of information technology and communications infrastructures. It is the goal of this paper to provide a foundation for States to build a better understanding not only of smart grid, but also of the cyber risks associated with smart grid, as well as options for addressing those risks, within the context of energy assurance planning.

In 2009, forty-eight States received American Recovery and Reinvestment Act (ARRA) funding from the U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) to institutionalize energy assurance planning. The purpose of this funding was to enable States to create or update their energy assurance plans and to provide for exercises and training associated with these plans. In the following passage, the DOE Funding Opportunity Announcement[2] details the initiative:

---

[1] DOE/OE, *Enabling States and Localities to Improve Energy Assurance and Resiliency Planning*, September 2010. See www.naseo.org/energyassurance/EAP_Brochure.pdf.

[2] Funding Opportunity Number: DE-FOA-0000091 Announcement Type: Amendment 002 CFDA Number: 81.122 Issue Date: 07/27/2009. See http://naseo.org/foa/energyassurance/OE_EA_FOA_Final_0000091_0021.pdf.

"Since the goal of the American Recovery and Reinvestment Act of 2009 (ARRA), in part, is to: "facilitate recovery from disruptions to the energy supply" and "enhance reliability and quicker repair of outages," this initiative will create jobs at the State level and allow States to have well-developed, standardized energy assurance and resiliency plans that they can rely on during energy emergencies and supply disruptions. State governments will address energy supply disruption risks and vulnerabilities in their plans to lessen the devastating impact that such incidents have on the economy and the health and safety of citizens.

This initiative, called "Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency Initiative" focuses on developing new, or refining existing, plans to integrate new energy portfolios (renewables, biofuels, etc) and new applications, such as Smart Grid technology, into energy assurance and emergency preparedness plans. Better planning efforts will help contribute to the resiliency of the energy sector, including the electricity grid, by focusing on the entire energy supply system, which includes refining, storage, and distribution of fossil and renewable fuels. The plans will address how States will respond to and recover from energy emergencies and reduce risks and vulnerabilities and build a more resilient energy infrastructure.

The ARRA initiative cited the *State Energy Assurance Guidelines*[3] as a model that states may use to develop their Energy Assurance plans. These Guidelines were developed by the National Association of State Energy Officials (NASEO) in collaboration with the National Association of Regulatory Utility Commissioners (NARUC) and funded by DOE/OE. The guidelines recognize that States need to increase awareness of smart grid and cyber security and integrate that awareness into their energy assurance planning efforts.

In support of the *State Energy Assurance Guidelines* and the States' energy assurance activities, this paper is organized in three principle parts:

1. An overview of the smart grid, the process for developing a smart grid, and examples of smart grid applications and their benefits with particular focus on energy assurance.
2. Guidance for State officials to assess the status of smart grid deployment in their States as part of their longer term energy assurance plans.
3. A step-by-step approach to building cyber security capability at the State level. NASEO recommends that this capability be developed and sustained in State energy agencies, as this is an issue that will continue to grow in importance.

This document is intended to provide guidance to State energy agencies—including State energy offices and public utility commissions—on potential roles, ideas, and areas to consider in the planning process. It is not intended to be prescriptive or exhaustive. The guidance should be used as appropriate, depending on the level of smart grid investment and cyber security development in a State. For States with

[3] *State Energy Assurance Guidelines*, Version 3.1, December 2009, See http://www.naseo.org/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf.

little to no smart grid or cyber security activity, a brief description of potential future activities may be sufficient for their energy assurance plans.

Finally, this guidance is provided with the expectation that State regulatory approaches on cyber security do not inhibit smart grid implementation. Rather, it suggests that States develop the capability to build and maintain a knowledge base of existing and developing standards to help assure their appropriate implementation and to assure that the potential benefits of smart grid are realized as those investments are made.

Section 2 – What is Smart Grid?

The smart grid as defined here is based upon the descriptions found in the Energy Independence and Security Act of 2007 (EISA 2007).[4]

The term "smart grid" refers to a modernization of the electricity infrastructure to maintain a reliable and secure system that can meet future growth. It is important to note that the smart grid vision is characterized by a two-way flow of electricity and information that creates an automated, widely-distributed electricity network. It will monitor, protect and automatically optimize the operation of its interconnected elements—from both central and distributed generators, through the high-voltage transmission network and the distribution system, to industrial users and commercial building automation systems; to energy storage installations; and to residential consumers with their thermostats, electric vehicles, appliances and other household devices.

Development of the smart grid will evolve over several years, and therefore it should be thought of as the development of a "smarter" grid. The smarter grid will incorporate information technology, sensors, and distributed computing to collect and analyze data to deliver real-time information. This information will be used to instantly match electricity demand with supply from all available sources, incorporating both traditional generation and wind, solar and electricity storage. The smart grid will enable a "just in time" balance of supply and demand at the device level.

This definition of the smart grid builds on work done in both the public and private sector, including EPRI's IntelliGrid[5] program, the Modern Grid Initiative,[6] and the GridWise Architecture Council.[7] These significant efforts have developed and articulated the vision statements, architectural principles, barriers, benefits, technologies and applications, policies, and frameworks that help define the smart grid. DOE captured the essence of these programs in *Smart Grid: An Introduction.*[8]

An excellent source of smart grid information and reference materials, DOE's *Smart Grid Information Clearinghouse*[9] provides resources for those just getting started with smart grid, as well as for those familiar with the concepts, methodologies, standards, and applications.

---

[4] Energy Independence and Security Act of 2007. See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf.

[5] EPRI IntelliGrid website. See http://intelligrid.epri.com/default.asp.

[6] Modern Grid Initiative website. See http://www.netl.doe.gov/smartgrid/.

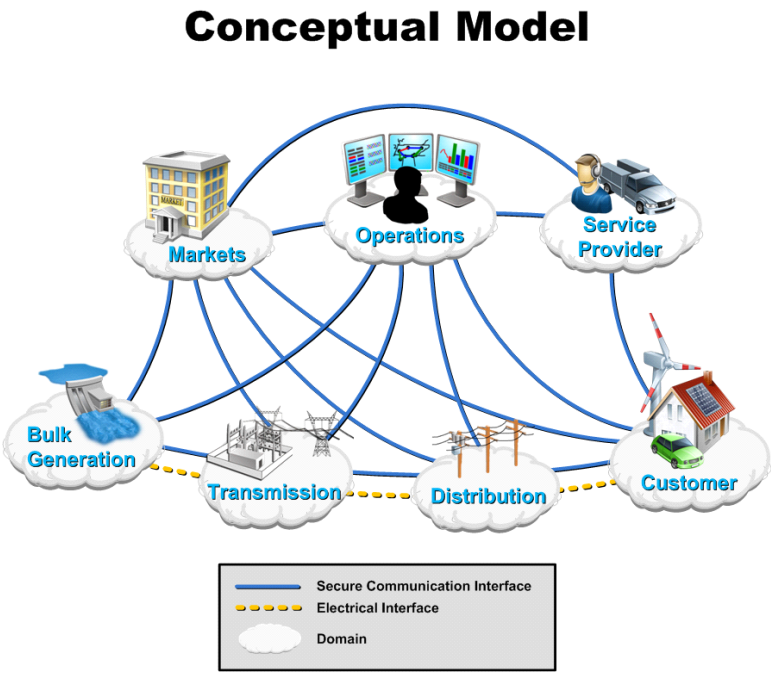
[7] GridWise Architecture Council website. See http://www.gridwiseac.org/.

[8] Smart Grid an Introduction Website. See http://www.oe.energy.gov/SmartGridIntroduction.htm.

[9] Smart Grid Information Clearing House website. See http://www.sgiclearinghouse.org.

Figure 1 provides a conceptual model of the smart grid. It consists of seven domains, each of which contains many technology applications. This model was designed by electricity stakeholders in their effort to provide input on smart grid interoperability to the National Institute of Standards and Technology[10] for the development of the smart grid interoperability standards roadmap. The diagram is a simplified model of the multiple and complex systems of smart grid.

Figure 1



Potential Benefits of Smart Grid

Potential smart grid benefits are categorized into the following five types. The energy assurance benefits are emphasized below. These benefits describe the vision of the fully-developed smart grid; actual benefits will be a function of selected smart grid applications and investment levels.

- **Power reliability and quality**: The smart grid provides a reliable power supply with fewer and briefer outages, higher quality power, and self-healing power systems through the use of digital information, automated control, and autonomous systems. The smart grid is resilient, but when an outage does occur, it recovers faster in emergencies and limits the extent of outages.

[10] Electric Power Research Institute *Report to NIST on the Smart Grid Interoperability Standards Roadmap (Contract No. SB1341-09-CN-0031—Deliverable 10), Post Comment Period Version Document,* Palo Alto, CA: June 17, 2009. See http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf.

- **Safety and cyber security benefits**: The smart grid continuously monitors itself to detect unsafe or vulnerable situations that could detract from its high reliability and safe operation. Cyber security features need to be built into all systems and operations, including physical plant monitoring, access control for confidentiality, integrity, and privacy protection of customer data.

- **Energy efficiency benefits:** The smart grid is more efficient, reducing energy consumption, peak demand, and energy losses in transmission and distribution systems. Such efficiencies can help to defer the construction of new centralized generation plants to meet electricity demand. An efficient grid is a more resilient grid: diverse supply and demand-side options provide operational flexibility. Less dependence on supply-side resources provides increased resilience.

- **Environmental and conservation benefits**: A smart grid will aid in reducing greenhouse gases and other emissions by managing the network to access efficient and low-emission energy sources, reliably integrating variable renewable energy sources, and enabling the replacement of gasoline-powered vehicles with plug-in electric vehicles. Integrating diverse supply options increases the resiliency of the grid.

- **Direct financial benefits**: The smart grid offers economic benefits. While smart grid developments require capital investment, programs must be designed so that benefits outweigh costs over a suitable time period. Customers will have pricing choices and access to energy information to manage energy use for financial benefit. Entrepreneurs will accelerate technology introduction into the energy generation, distribution, and storage markets. Increased reliability and power quality may also result in financial benefits to electricity generators and local distribution utilities.

To fully understand these benefits, it is useful to explore further how they contribute to: the integration of renewable energy into the power grid, and provide for "self-healing" capabilities, which in turn contribute to improved reliability, resiliency, and power quality.[11]

Integrating Renewable Resources. As noted earlier, smart grid enables the integration of variable renewable energy resources, such as wind, hydro, and solar energy, to supply power to the grid when the energy is available. Traditionally, the problem with some sources of renewable energy, particularly wind and solar photovoltaic (PV) energy, has been that they may supply power intermittently causing rapid power fluctuations on the grid. When the variable energy resource is

---

[11] For more details on the benefits of the Smart Grid see: "*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 2011. See http://www.sgiclearinghouse.org/node/3272.

not available, other sources must be ready to meet demand. Alternatively, to maintain system reliability, demand must be reduced to match the available supply.

The smart grid will enable the integration of variable energy supply and maintain system reliability by monitoring and predicting variable supply resources. It will be able to automatically bring in other power supply resources to meet demand, or reduce load to match the supply. The smart grid will use sensors, such as synchrophasors and dynamic line rating systems, to enhance the visibility and monitoring of the transmission grid and to maintain and potentially improve its reliability in the presence of large variable sources of electricity. Modern computing applications will receive and analyze real time information and perform modeling, decision-making, and controlling actions. Instead of control devices operating independently based on local measurements, networked smart grid applications will analyze data from multiple devices, allowing broader and more coordinated operations that adapt to actual situations and stabilize the grid.

The smart grid also addresses transmission congestion created by insufficient transmission capacity. Such congestion drives up overall bulk power costs. By managing congestion, the smart grid can ensure that remotely located wind generation is not constrained from reaching load centers.

Self-Healing Power Grid. The concept of "self-healing" means that the grid detects problems in real time, isolates the problem, and keeps the grid operating during emergencies. Currently, power grids may experience cascading failures in emergency situations where outages are poorly contained. The technologies for containing cascading failures continue to dramatically improve, and are being implemented on the bulk power system to lessen this vulnerability. On the policy side, however, conventional methodology for emergency control is based on State-specific operating rules derived from off-line studies that determine local emergency automation schemes, locations, and settings. The scope of these rules is limited to responding to a pre-determined menu of conditions rather than diagnosing exigent circumstances. The smart grid may improve the evaluation of power system behavior in real time, prepare the power system to withstand credible combinations of contingencies, prevent wide-area blackouts, and accommodate fast recovery from emergency to normal conditions. The smart grid will utilize fast-simulation and modeling tools to gather information, model, make decisions and control actions. The tools will be located in a combination of central and widely distributed positions.

In an emergency outage situation, the self-healing smart grid provides the capability to isolate the problem areas while keeping the rest of the grid operating and avoiding cascading failures. The problem areas can be repaired and restored with minimal impact on the wider area. The future control system for the self-healing grid will differ from current approaches. Instead of supervisory controls by operators, smart grid will implement significantly more automated controls. It will aim toward the preservation of adequate integrity of the generation-transmission-distribution-customer system rather than the self-protection of equipment only. While many of these capabilities have already been deployed in some parts of the bulk power system, the smart grid holds the promise of bringing this level of control and

reliability more evenly across regions and more deeply and effectively on the electric grid.

Smart Grid Applications

The smart grid uses enabling technology to achieve specific objectives. Smart grid technologies include advanced sensors, system communication infrastructure, advanced power delivery equipment and controls, and advanced modeling and simulation techniques. The following applications of smart grid are examples of how smart grid technology can be used. A smart grid must be *designed* to run desired applications; smart grid deployments will not run all the following applications unless designed to do so.

Distribution Grid Management – Distribution power systems consist of hundreds of distribution feeders and thousands of distribution transformers that supply millions of customers. They also contain a large number of locally and remotely controllable devices. Distribution power systems are large and complex systems to control. Basic modernization that includes distribution automation and control systems as well as smart grid technologies will enable distribution systems to be more fully automated, capable of self-healing, and optimized to reduce losses.

- **Outage management/recovery**: Smart grid technologies can significantly enhance outage detection, providing near instantaneous detection, a capability not currently available to distribution system operators. Information will be available on when and where outages have occurred, and will contribute to determining causes of outages. Recovery time will be minimized and outages will have reduced impacts on consumers. Information will be available to track consumers without power and restoration rates.

- **Voltage optimization/conservation; voltage reduction**: Optimizing the voltage of a distribution line can help to reduce distribution line losses and the energy consumption of some consumer equipment with no effect on performance. Many loads operate more efficiently at lower voltage. With voltage optimization, voltages are optimized to loads, so that they operate as efficiently as possible with minimal disruptions. Smart grid equipment on the system, such as distributed sensors, control capacitors, and regulators will provide capabilities to optimize voltage. Advanced metering will provide voltage information on the consumer premises.

- **Other smart distribution system applications:** Other applications include fault detection, characterization, and location; automatic system reconfiguration (self-healing); and equipment and system diagnostics.

Advanced Metering Infrastructure – Advanced metering infrastructure (AMI) provides two-way communication between the utility and the consumer. AMI enables dynamic pricing of electricity that more closely matches marginal cost with price throughout the day. The utility receives information about consumer electricity

usage, such as near real-time usage, load shapes and peak demand usage. The meter can also supply voltage data for voltage optimization and outage tracking. The consumer receives near real time information about electricity use on the premises and enables dynamic pricing.

- **Empowering consumer management and use of electricity:** Information to the consumer displayed in an understandable way helps empower the consumer to manage and control electricity use to meet productivity, cost, and environmental goals. Consumers will use the "Prius effect" – a phenomenon of Toyota Prius drivers learning to optimize their driving by monitoring their energy usage on the dashboard display. This will enable consumers learn how to reduce bills by, for example, turning equipment to lower energy settings – or completely off – when not needed, and unplugging "vampire" loads, such as electronic device chargers, when not in use.

- **Demand response:** With peak demand pricing, advanced metering infrastructure, energy management capability, and smart appliances, consumers can take advantage of "prices to devices." This concept enables consumers to take control of their electricity use when it matters most – when prices rise during peak demand periods. Consumers can pre-program their energy management systems or smart appliances to operate within selected price and performance levels. When high prices arrive, the system reacts automatically as directed by the consumer, by turning equipment down, (such as the air conditioner in a commercial building), stopping operation of certain functions, (such as the defrost cycle on the freezer in a home), or not operating at all, (such as a residential pool pump or a commercial building fountain).

- **Consumer education:** The capabilities provided by advanced meter infrastructure bring new approaches for consumers. Educational programs will help consumers confidently take advantage of new features, services, and rate and price offerings to improve their own use and management of their electricity consumption.

Section 3 – Smart Grid for Energy Assurance Planning

This section provides guidance to States on how to incorporate smart grid concepts into energy assurance planning. The initial goal is to define how the smart grid contributes to the main objectives of energy assurance enabling more rapid restoration of power after outages, building resiliency, enhancing reliability and security, and reducing risk and vulnerability.

Energy assurance planners must begin with a broad, high-level understanding of the current status of smart grid activities in the State and how these various efforts interrelate and contribute to the goals of energy assurance. This includes familiarity with not only the utilities' role and future plans, but also consideration for the contributions of other stakeholders, such as manufacturers of smart appliances or the State and Federal governments that promote smart grid deployment through programs, policies and funding.

Assessing the Status of State Smart Grid Developments

The first step in addressing smart grid as part of State energy assurance plans is to understand the current level of activity and investment in the State. Key questions include: what has been done, where and what types of investments have been made, and what projects and investments are planned for the future. Answers to these questions may be closely related to the activities that some States have begun under the State Electricity Regulatory Assistance Grant for Smart Grid, an ARRA DOE/OE funded grant given to State pubic utility commissions. Any intersection between this work and State energy assurance plans should be identified and coordinated.

What follows is an outline that States can use in whole or in part, or as a starting point for further modifications, within a State energy assurance plan. Some States may require more technical details, and some may require fewer; this should be tailored to the needs of the State.

1. Describe the current status of smart grid implementation:
    a. Purpose(s) and drivers for smart grid projects.
        i. Energy assurance aspects; emergency response, resiliency and risk mitigation.
        ii. Business case developed by utilities and others.
        iii. Other expected benefits.
    b. Overall plan for smart grid implementation; technologies installed and planned.
    c. Degree to which smart grid implementation has enabled or will enable:
        i. Improvements in security, reliability and resiliency.
        ii. More rapid recovery from power outages.
        iii. Demand management and energy efficiency programs.
        iv. Integration of distributed generation and renewable energy.
        v. Integration of plug-in electric hybrid vehicles.
        vi. Use of smart grid distribution automation.

d. Plans for evaluating performance and benefits, and comparing to initial estimates.
e. Digital meters (also known as smart meters and advanced metering infrastructure (AMI)).
    i. Overview of meter investment plan, objectives, drivers.
    ii. Relation to energy assurance plans.
    iii. A description of the meter functional capabilities (the type of meter deployed may vary among utilities).
    iv. Number and location of AMI/smart meters installed.
    v. Implementation of meter data management systems to support the large volume of data and make it available to other utility processes.
    vi. Customer web portal for customers to access and view their own usage from as recent as prior day.
    vii. Two-way communications through the AMI and related head-end management systems to provide services to customers, such as demand response and pre-pay services.
    viii. Determination of whether the systems being deployed proprietary or standards or open-source based systems.
    ix. Integration of meter outage notifications into utility outage management systems, to better and more rapidly identify the number and location of customers affected and the rate of recovery.
f. Distribution system.
    i. Overview of distribution system investment plan, objectives, drivers.
    ii. Relation to energy assurance plans.
    iii. Automated and remotely controlled capacitor banks for var (reactive power) and power factor control, to maintain voltage on feeders at optimum levels to save end-use energy and to reduce losses.
    iv. Supervisory-controlled reclosers to speed restoration for faults that clear themselves, avoiding manual fuse replacements.
    v. Automated fault isolation and feeder reconfiguration equipment.
    vi. Mobile workforce management systems that dispatch crews already in the field to new work assignments, such as outage repairs, in a timely and effective manner.
    vii. Outage management systems that integrate smart meter "last gasp" outage information for better and more rapid identification of the number of customers affected (and their location) to speed restoration of power.
    viii. Distribution management systems that incorporate seamless interface for operators and provide for fault location to speed crews to precise locations of outages.
g. Transmission system.
    i. Overview of transmission system investment plan, objectives, drivers.

ii. Relation to energy assurance plans.
iii. Phasor measurement units[12] (PMUs) at key grid nodes.
iv. Dynamic line rating tools and methods for system operators.
v. Condition monitoring of major transformers to allow operation at maximum safe loadings and detect emerging equipment problems.

2. Describe utility and other State and private sector plans for future smart grid deployment, including pilot and demonstration programs. Describe both future projects, including near term and the longer term. The description should include the level of investment and other factors driving deployment, such as laws and regulatory requirements, reliability, security, operational efficiency, etc:
    a. The level and source of investments, including those funded by grants, stockholders, and those already approved by the State utility commission for inclusion in rates.
    b. Are there future investments which are pending approval?
    c. Any non-utility smart grid related investments that may integrate into the smart grid. For example, this could include storage for renewable projects such as compressed air, battery, pumped hydro, etc.
3. Identify any State public utility commission orders or administrative rules addressing smart grid, and any special conditions that may have been set by the commission.
4. Identify any pending cases that address smart grid in whole or in part.
5. Identify any future anticipated cases that may address smart grid investment.
6. Identify any projects that may be funded by other sources that may support smart grid, including the State Energy Program or the Energy Efficiency Conservation Block grants to local communities.

This outline is not meant to be a definitive list of topics and there are other ways to organize the information on smart grid activities in each State. One alternative is to arrange and organize the information using the categories of smart grid projects identified by the Grid Wise Alliance, see http://www.gridwise.org/.

[12] Phasor Measurement Unit - Synchronized phasor measurements—also known as phasor measurement units (PMUs)—are ideal for monitoring and controlling dynamic power system performance, especially during high-stress operating conditions.PMU applications—The five major applications include 1) improvement on state estimation, 2) oscillation detection and control, 3) voltage stability monitoring and control, 4) load modeling validation, and 5) system restoration and event analysis. See http://www.naspi.org/.

Section 4 – Cyber Security for Smart Grid

Cyber security for the electric sector is a national concern. The concern is growing as the power system becomes increasingly complex and reliant on information technology and communications infrastructures. This reliance has seen a corresponding increase in the power system's vulnerability to cyber attacks. The management and protection of these infrastructure systems and components should be addressed as part of energy assurance plans because of the potential for power outages caused by cyber attack.

The role of cyber security in ensuring the effective operation of the smart grid is documented in Federal legislation. As stated in the EISA 2007, the first two referenced characteristics of smart grid address security:

> *(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.*
>
> *(2) Dynamic optimization of grid operations and resources, with full cyber security…*[13]

Cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cyber security also includes restoring electronic information and communications systems in the event of a deliberate attack or natural disaster.[14]

Cyber security must address deliberate attacks, such as those launched by disgruntled employees, industrial espionage, terrorists and sovereign nation states. It also needs to prevent inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters.

Security is best applied in layers and at different levels. The term "layers" implies multiple security barriers between the attacker and the target, while the term "levels" refers to the different levels in the communications infrastructure underlying any cyber system. This concept is referred to as "defense in depth."

Defense in depth is a critical concept that can be illustrated by the following:

- If one security barrier is broken, such as the lock on a door, the next layer may prevent the attack. For example, the attacker who gains access through a door with a broken lock will be slowed or stopped if he does not have the correct password. This level may deter the attacker until the attack is detected, such as by video surveillance or an alarm signifying that an excess of passwords has been attempted.

---

[13] EISA 2007. See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf.

[14] US Department of Homeland Security. See http://www.dhs.gov/files/programs/editorial_0827.shtm#0 (National Infrastructure Protection Plan. See http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

- The system may detect the attack and it may trigger responses to the attack, such as a lock-down of all access to the attacked facilities.
- The system may mitigate the damage to equipment (e.g., by breakers tripping off), or it may allow the system to continue to operate during an attack via automated switching to restore most power immediately.
- The system may help restore power via black start capability. It may also help investigators to understand the source of the attack, and even prosecute the attacker, by using audit logs to determine exactly which actions were taken, when, and by whom.

A cyber security strategy will take into account information on impacts, vulnerabilities, and threats to produce a risk assessment. In a typical risk management process, assets, systems and networks are identified; risks (including vulnerabilities), impacts and threats are assessed; cyber security requirements are specified; and cyber security controls are selected, implemented, assessed for effectiveness, authorized, and then monitored over the lifecycle of the system.

Development of Cyber Security Capability at the State Level

Cyber security is not a one-time activity like building a fence for protection. Because smart grid will be built over time, cyber security must also grow over time to address threats and vulnerabilities in the short term as well as the longer term. While the focus of this paper is smart grid, many of the security practices it outlines apply to the entire energy sector and to the day-to-day operations of all organizations. The development of this capability can be used to address the need in these other areas as well. For additional background information on cyber security see the NASEO/NARUC *Energy Assurance Guidelines* (pages 23 to 29).[15]

As a precursor to this effort, it is important for States to understand the nature of the risk and the threat of cyber attacks. Examples of cyber attacks include the following:

- In 2001, hackers penetrated the California Independent System Operator, which oversees most of the State's electricity transmission grid; attacks were routed through California, Oklahoma, and China.
- Ohio's Davis-Besse nuclear power plant safety monitoring system was offline for five (5) hours due to the Slammer worm in January 2003.
- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities electronic control systems.
- In April 2009, the Wall Street Journal reported that spies hacked into the U.S. electric grid and left behind computer programs that could allow them to disrupt service.

[15] NASEO Energy Assurance Guidelines. See http://www.naseo.org/eaguidelines.

- Associated Press on August 4, 2010 reported "Hackers Try to Take over Power Plants." In September 2010, cyber experts discovered for the first time a malicious computer code, called a worm, specifically created to take over systems that control the inner workings of industrial plants.
- The Stuxnet Worm was reported in an Industrial Control Systems Cyber Emergency Response Team Advisory on September 29, 2010. Stuxnet is a Malware Targeting Siemens Control Software. It can be used to infiltrate industrial control systems used in the power grid, power plants and other infrastructure. It is reported to have the ability to damage or possibly destroy control systems.
- The North American Electric Reliability Corporation (NERC) and DOE released a report titled *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (June 2, 2010)[16] that identifies a certain class of high-impact, low-frequency risk shown to have the potential to significantly affect the reliability of the North American bulk power system. The report examines three high-impacts, low-frequency risks in detail: coordinated cyber, physical, or blended attacks; pandemic illness; and geomagnetic disturbances and electromagnetic pulse (EMP) events.
- NERC issued a recommendation[17] to industry on the AURORA vulnerability[18] in October 2010. The recommendation provides new sensitive and clarifying information regarding the nature of AURORA. The recommendation requires entities to report on efforts and progress by Dec. 13, 2010 with updates every six months until mitigation is complete.

A critical prerequisite to this effort is for State energy offices and public utility commissions to recognize the importance of cyber security and assign staff resources to cyber security on an ongoing basis. This might also be done using a team or task force approach. Cases before public utility commissions on cost recovery of smart grid investments should explore the degree to which these investments have met or exceeded the existing and potentially future cyber security requirements as described in the following sections.

The National Association of Regulatory Commissioners (NARUC) adopted a *Resolution Regarding Cyber Security*[19] in February 2010. This resolution encourages

---

[16] High-Impact, Low-Frequency Event Risk to the North American Bulk Power System NERC, June 2010 See reference, http://www.nerc.com/news_pr.php?npr=587.

[17] NERC Issues Aurora Alert to Industry, Oct. 14, 2010. See http://www.nerc.com/fileUploads/File/PressReleases/PR_AURORA_14_Oct_10.pdf.

[18] In 2006, Idaho National Laboratory demonstrated spinning machine connected to the power grid -- such as a generator, pump or turbine could be destroyed by attacks carried out on vulnerable equipment using the Internet to exploit cyber vulnerability. This became known as the AURORA vulnerability.

[19] NARUC Resolution Regarding Cyber Security, February 2010. See http://www.naruc.org/Resolutions/Resolution%20on%20Cybersecurity1.pdf.

commissions to open a dialogue with their regulated utilities to ensure that these organizations are in compliance with standards, and where applicable, ensure that cost-effective protection and preparedness measures are employed to deter, detect, respond, and recover from cyber attacks. It also encourages commissions to regularly revisit their own cyber security policies and procedures to ensure that they are in compliance with applicable standards and best practices, such as those of the National Institute of Standards and Technology (NIST) and Certification for Information System Security Professionals (CISSP). State energy offices and other agencies with energy assurance responsibilities should do the same. The resolution also states in part:

> *"That NARUC supports member commissions in becoming and remaining knowledgeable about these threats, and ensuring that their own staffs have the capability, training, and access to resources to adequately review and understand cyber security issues that enhances expertise in the review of cyber security aspects of filings by their jurisdictional utilities…"*

In addition to committing staff resources, States should provide training for cyber security to assure a sufficient depth of knowledge as needed. While some State public utility commissions and state energy offices may elect to employ individuals with cyber security expertise, they should at a minimum maintain staff that is sufficiently knowledgeable to be able to ask the right questions and fully understand the cyber security measures taken by utilities. State public utility commissions should understand to what degree utilities they regulate meet or exceed guidelines and standards that exist or may be adopted in the future.

Once staffing has been committed, the following is an approach (set of steps) that could be taken as one path to build this capability. This approach suggests an understanding of cyber security in the workplace as a primary step toward developing an understanding of cyber security practices. If the staff knowledge level is beyond this point, then move directly to Step 2.

Step 1 – Understand the State's internal cyber security profile.

1. Understand cyber security risks at work and at home. Many States and organizations have guidance available. For an example see: http://www.michigan.gov/cybersecurity.
2. Identify the individuals in the State who have the primary roles for addressing cyber security, and identify their roles and responsibilities.
3. Determine which State agency, if any, has lead and/or supporting roles and responsibilities in cyber security as it directly relates to smart grid implementation.
4. Become familiar with the State's Continuity of Operations Plans (COOP)[20] and disaster recovery strategies that pertain to the essential cyber security systems.[21]

[20] FEMA Continuity of Operations. See http://www.fema.gov/government/coop/index.shtm.

5. Determine if it may be helpful to become a member of the FBI's InfraGard Program: http://www.infragard.net/.
6. Become familiar with the U. S. Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber attacks for the Federal Civil Executive Branch, as well as information sharing and collaboration with State and local government, industry and international partners. See http://www.us-cert.gov/.

Step 2 – Understand the *current* cyber security requirements for the energy sector.

1. Electricity and smart grid:
    a. NERC -- Standards CIP-002 through CIP-009 (the Critical Cyber Asset Identification portion of the Critical Infrastructure Protection Standards[22].
    b. Section 1305 of EISA 2007 defines the roles of both Federal Energy Regulatory Commission (FERC) and NIST as they relate to the development and adoption of smart grid standards. Subsection 1305(d) defines the Commission's role. This subsection reads as follows: "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."[23]
2. Understand the cyber security requirement for other parts of the energy sector including natural gas (pipeline safety standards) and the petroleum sector, because of the interdependency effects that need to be considered.
3. Under EISA 2007, NIST has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"
    a. The NIST Smart Grid Interoperability Standards Project[24] is working to meet this goal.
    b. One of the primary documents was issued in January 2010 and titled *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0 (Framework)."[25]

---

[21] The SANS (SysAdmin, Audit, Network, Security) Institute. See http://www.sans.org/reading_room/whitepapers/recovery/.

[22] See: http://www.nerc.com/page.php?cid=2%7C20.

[23] Ray Palmer Smart Grid Update to FERC A-3: (Docket No. AD10-15-000) July 15, 2010.

[24] Smart Grid Interoperability Standards Project. See http://www.nist.gov/smartgrid/.

[25] National Institute of Standards and Technology (NIST) *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, January 2010. See www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

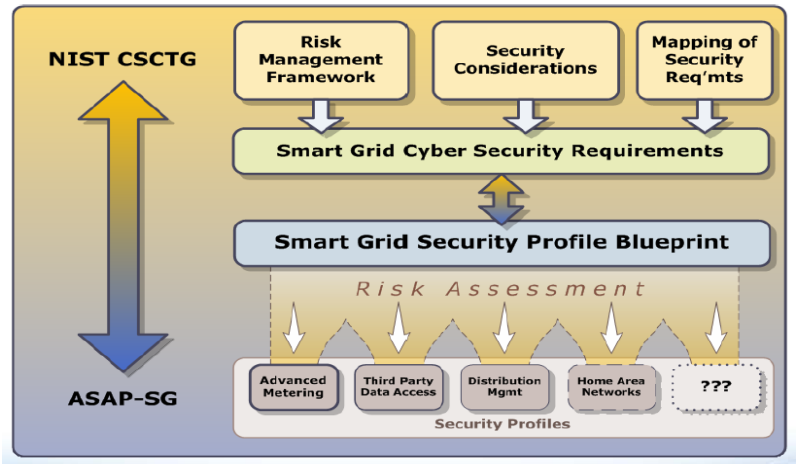
c. The Framework identified 75 interoperability standards that are applicable, or are likely applicable, to the ongoing development of smart grid technologies and applications.[26]
d. NIST developed *Guidelines for Smart Grid Cyber Security.*[27]

Step 3 – Understand ***future*** standards and guidelines currently under discussion and development, and how they may affect utilities' plans for smart grid deployment.

1. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) is a utility-driven, public-private collaborative among DOE, EPRI, and a large group of leading North American utilities. ASAP-SG is developing system-level security requirements for smart grid applications, such as advanced metering, third party access for customer usage data, distribution automation, home area networks, and synchrophasors. ASAP-SG is capturing these requirements in a series of Security Profiles, which are submitted to the SG Security Working Group within the UCA International Users Group (UCAIug) for ratification. ASAP-SG also submits the Security Profiles to the Cyber Security Working Group (CSWG) as input in development of the Guidelines for Smart Grid Cyber Security[28].

   As a result of the collaboration between the CSWG and ASAP-SG, the *Guidelines for Smart Grid Cyber Security* provide context and establish logical interface categories for the ASAP-SG Security Profiles, while the Security Profiles in turn provide detailed, actionable, and tailored controls for those building and implementing specific smart grid systems. See Figure 2.

Figure 2



[26] Ray Palmer Smart Grid Update to FERC A-3: (Docket No. AD10-15-000) July 15, 2010.

[27] National Institute of Standards and Technology (NIST), NISTIR 7628 *Guidelines for Smart Grid Cyber Security*, Introduction and Volumes 1-3, The Cyber Security Coordination Task Group, Advanced Security Acceleration Project Smart Grid, August 2010. See http://csrc.nist.gov/publications/PubsNISTIRs.html.

[28] Ibid.

To date, ASAP-SG has produced three Security Profiles.

a. The Security Profile for Advanced Metering Infrastructure (*AMI Security Profile*) has been ratified by the AMI-SEC Task Force within the UCAIug and provides prescriptive, actionable guidance for how to build in and implement security from the meter data management system up to and including the home area network interface of the smart meter. The AMI Security Profile served as the basis for early discussions of security for advanced metering functions, eventually informing selection of requirements for the various Logical Interface Categories.
b. The Security Profile for Third Party Data Access (*3PDA Security Profile*) has been ratified by a Usability Analysis team within the UCAIug SG Security Working Group. It delineates the security requirements for individuals, utilities, and vendors participating in three-way relationships that involve the ownership and handling of sensitive data (e.g., electric utility customers who want to allow value-added service providers to access electric usage data that the utility serving the customer possesses). The 3PDA Security Profile served as a reference point for many discussions on the subject of privacy, and informed several aspects of Chapter Three – Privacy and the Smart Grid of the *Guidelines for Smart Grid Cyber Security*.
c. The recently completed Security Profile for Distribution Management (*DM Security Profile*) has been handed over to the SG Security Working Group for review and ratification, and addresses automated distribution management functions including steady state operations and optimization. For this profile, "distribution automation" is treated as a specific portion of distribution management related to automated system reconfiguration and Supervisory Control and Data Acquisition (SCADA), and is within scope.

Publicly available versions of ASAP-SG documentation may be found on SmartGridiPedia at http://www.smartgridipedia.org.

2. The National Electric Sector Cyber Security Organization (NESCO) is leading a broad-based, public-private partnership focused on cyber security. NESCO unites asset owners, vendors and manufacturers, the academic community, and government together with a common purpose: to improve electric sector cyber security. NESCO is operated by EnergySec with funding support from the U.S. Department of Energy. It is a three-year public-private partnership that is laying the foundation for what is expected to be a self-sustaining organization in the future. NESCO serves as the focal point to bring together domestic and international experts, developers, and users who assess and test the security of novel technology, architectures, and applications. In addition, the organization focuses on monitoring, collection,

analysis, mitigation, and dissemination of infrastructure security vulnerabilities and threats.

NESCO, building upon the EnergySec information sharing foundation, has developed and implemented technology to facilitate enhanced information sharing among and between the four participant groups. NESCO is also building out a rapid notification system to provide information of threats and vulnerabilities quickly to those that may need to respond. NESCO supports cyber security solutions development, especially in the areas of open source technologies. Currently under development is a code and best practices repository. Plans were rolled out for a "Tactical Analysis Center" recently as well. The Tactical Analysis Center is an industry driven program focused on security issues relevant to the sector. It serves as the primary outlet for advisories, pass-through alerts, and industry-specific analysis of rapidly developing security information.

The National Electric Sector CyberSecurity Organization Resource (NESCOR) serves in a supporting role to NESCO. NESCOR is comprised of a team of partners and experts led by EPRI to assist NESCO in creating a framework to identify and address immediate and future challenges for securing the electricity sector. Partners include Oak Ridge National Laboratory, Idaho National Laboratory, National Renewable Energy Laboratory, Sandia National Laboratories, Palo Alto Research Center, Telcordia, SRI, University of California Berkeley, University of California Los Angeles, University of Minnesota, University of Houston, and several subject matter experts and cyber security consultants in the power industry. While NESCO focuses on the tactical and operational aspects of cybersecurity, the focus of NESCOR lies more in the areas of research and regulation.

NESCOR is divided into three working groups, each with a different focus. The Threat and Vulnerability Assessment and Mitigation team focuses on the development of mitigation strategies for identified vulnerabilities in the sector. The Cybersecurity Requirement and Standards Assessment team assesses cyber security requirements and standards from NIST, DHS, NERC, UCA and other entities to determine how well the current standards are meeting those requirements. The Cybersecurity Technology Testing and Validation working group focuses on the development of methodologies and testing plans for emerging technologies that could provide cyber security protections.

Step 4 – Determine whether there are cyber security plans in place, and whether they are driven by State regulatory or Federal grants compliance.

In addition to the requirements for the electricity grid that are standards-driven, it's also important to understand those requirements that are non-standards driven. Such standards may be subject to regulation or to compliance with DOE Smart Grid

Investment Grant criteria. For the former, plan-writers may want to determine whether there are regulatory efforts underway at a State utility commission to create audit, reporting and compliance obligations on cyber security for the utilities. Examples of such obligations include the self-certification of cyber security measures employed by the Pennsylvania Public Utility Commission and the notices of inquiry that have been implemented in Missouri. Commission staff in Pennsylvania, however, does not inspect security plans or derive any system understanding other than the potential relative vulnerability level of specific distribution and transmission systems.

States need to identify the best options for working with the private sector to address cyber security concerns in general. This is an evolving issue that will change over time and will require attention to new and emerging concerns. While regulatory and compliance issues are part of what needs to be addressed, so are policy and program issues, as well as the way States address the public private partnerships as provided for in the National Infrastructure Protection framework[29] and the Energy Sector Specific Plan.[30]

The Smart Grid Investment Grants (SGIG)[31] program under the American Recovery and Reinvestment Act required utilities proposing projects to develop cyber security plans. It is recommended that any State with investment grant projects should become aware of what areas are covered by those plans. The SGIG grant language requires a description of how cyber security concerns will be addressed with respect to the use of best available equipment and the application of procedures and practices involving system design, testing, deployment, operations and decommissioning, including at a minimum:

1. A description of the cyber security risks at each stage of the system deployment lifecycle.
2. Cyber security criteria used for vendor and device selection.
3. Cyber security control strategies.
4. Descriptions of residual cyber security risks.
5. Relevant cyber security standards and best practices.
6. Descriptions of how the projects will support/adopt/implement emerging smart grid security standards.

---

[29] US Department of Homeland Security. See http://www.dhs.gov/files/programs/editorial_0827.shtm#0 (National Infrastructure Protection Plan. See http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

[30] US Department of Homeland Security Energy Sector Specific Plan. See http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf. Note the 2010 update became available in November 2010, but was not available on-line at the time this report was published.

[31] DOE/OE Smart Grid Investment Grants. See http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants.

Another area to consider is whether the cost to meet cyber security requirements will be recovered. Public utility commissions need to address how regulated utilities will pay for the necessary infrastructure upgrades to meet the cyber security requirements. This is a necessary step because of the ubiquitous presence of legacy information systems that will require upgrades to meet the cyber security requirements. The commissions need to work with the regulated utilities in their jurisdictions to determine the optimal migration plan. This plan should protect the consumer in terms of electricity reliability and costs, while keeping the utility operational limits and financial solvency in perspective. Commissions may wish to collaborate with EPRI in the NESCO program to determine the roadmap for compliance with current and future cyber security requirements.

Step 5 – Consider and address the human element of cyber security. While this is the final step, in many ways it is also one of the most important. It represents a serious ongoing vulnerability, and therefore it is critical to assure that it is properly addressed.

1. Understand what the insider threat is and what policies and procedures are in place to prevent intrusion and manipulation.
2. Understand what social engineering is and how it can be used to access systems.
3. Understand that technical solutions to security should account for human behavior, which can be driven by both cultural and psychological factors.
4. Understand the nature of the threat from employees, contractors, consultants, or anyone with short or long term access to information technology systems, and know about system vulnerabilities.
5. Understand that the effect of new systems on consumer behavior could be both a plus and a minus. It could strengthen security or incite actions to attack the system.

Section 5 – Conclusions

The smart grid can be a critical component of an energy-resilient infrastructure because the smart grid, if properly designed and implemented, should help ensure that electricity will continue to be highly reliable, used more efficiently, and will become increasingly more resilient. Smart grid characteristics that ensure these factors include the ability to:

- Anticipate and respond to system disturbances.
- Operate with resiliency to deliberate attacks and natural disasters.
- Accommodate all generation and storage options.
- Optimize asset utilization and operate efficiently.
- Address cyber security goals for availability, integrity, confidentiality, reliability and accountability.

The incorporation of smart grid and cyber security in State Energy Assurance Plans is an important means of documenting and building a greater understanding of the associated technologies and their implications. States are well advised to take a careful look at how smart grid and cyber security can support energy emergency response and build resiliency, reliability and security, while simultaneously meeting consumer and societal needs.

* * *

References and Resources

Smart Grid

Electric Power Research Institute*, 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* Palo Alto, CA: 2011. 1022519. See http://www.sgiclearinghouse.org/node/3272.

Electric Power Research Institute, *Integrating New and Emerging Technologies Into the California Smart Grid Infrastructure: A Report on a Smart Grid for California.* Palo Alto, CA and California Energy Commission (CEC), Sacramento, CA: 2008. 1018191. See http://www.energy.ca.gov/2008publications/CEC-500-2008-047/CEC-500-2008-047.PDF.

Electric Power Research Institute, *Report to NIST on the Smart Grid Interoperability Standards Roadmap (Contract No. SB1341-09-CN-0031—Deliverable 10), Post Comment Period Version Document,* Palo Alto, CA: June 17, 2009. See http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf.

Electric Power Research Institute, *Methodological Approach for Estimating the Benefits and Costs of Smart Grid Demonstration Projects*. Palo Alto, CA: 2010. 1020342. See http://www.smartgridnews.com/artman/uploads/1/1020342EstimateBCSmartGridDemo2010_1_.pdf.

Electric Power Research Institute IntelliGrid website. See http://intelligrid.epri.com/default.asp.

GridWise Architecture Council website. See http://www.gridwiseac.org/.

McGranaghan, M., Von Dollen, D., Myrda, P., Hughes, J., Electric Power Research Institute, *"Using the Intelligrid Methodology to Support Development of a Smart Grid Roadmap,"* Grid-Interop 2008, Paper C-138.

Modern Grid Initiative website. See http://www.netl.doe.gov/smartgrid/.

National Association of Regulatory Utility Commissioners (NARUC), *The Smart Grid: An Annotated Bibliography of Essential Resources for State Commissions May 2009.* See http://www.naruc.org/Publications/NARUC Smart Grid Bibliography 5_09.pdf.

National Institute of Standards and Technology (NIST) *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108,

January 2010. See http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Software Engineering Institute of Carnegie Mellon Smart Grid website: See http://www.sei.cmu.edu/smartgrid/.

U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability *Smart Grid: An Introduction 2008.* See http://www.oe.energy.gov/SmartGridIntroduction.htm.

Wakefield, M. and McGranaghan, M., Electric Power Research Institute, "*Achieving Smart Grid Interoperability through Collaboration,"* Grid-Interop 2008, Paper C-37.
"IntelliGrid Methodology for Developing Requirements for Energy Systems," International Electrotechnical Commission (IEC) Publicly Available Specification (PAS), IEC/PAS 62559, January 29, 2008. See http://webstore.ansi.org/RecordDetail.aspx?sku=IEC%2FPAS+62559+Ed.+1.0+en%3A2008.

Cyber Security

AMI-SEC Task Force *Advanced Metering Infrastructure (AMI) System Security Requirements*, December 2008. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology, 2007.* See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 2: Establishing a Manufacturing and Control Systems Security Program*, 2009. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Federal Bureau of Investigation, InfraGard program, *InfraGard FBI Cyber Security Collaboration*. See http://www.infragard.net/.

Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. See http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Idaho National Laboratory, *Cyber Assessment Methods for SCADA Security*, 2005. See http://www.naseo.org/eaguidelines/documents/cybersecurity/SCADA_Security.pdf.

National Institute of Standards and Technology (NIST), NISTIR 7628 *Guidelines for Smart Grid Cyber Security*, Introduction and Volumes 1-3, The Cyber Security Coordination Task Group, Advanced Security Acceleration Project Smart Grid, August 2010. See http://csrc.nist.gov/publications/PubsNISTIRs.html.

National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008. See http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf.

North American Electric Reliability Corporation (NERC), *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 2002. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Smart Grid Cyber Security Blog Spot. See http://smartgridsecurity.blogspot.com/.

U.S. Department of Homeland Security *National Infrastructure Protection Plan*, 2009. See http://www.dhs.gov/nipp.

U.S. Department of Homeland Security IT, telecommunications, and energy sectors sector specific plans (SSPs), and updated tri-annually. See http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) and the Energy Sector Control Systems Working Group, Roadmap to Achieve Energy Delivery Systems Cybersecurity, September 2011. See http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf.

U. S. Computer Emergency Readiness Team (US-CERT), U.S. Department of Homeland Security. See http://www.us-cert.gov/.

Other References and Resources

American Petroleum Institute *Security Guidelines for the Petroleum Industry,* April 2005. See http://new.api.org/policy/otherissues/upload/Security.pdf.

Idaho National Engineering and Environmental Laboratory *A Comparison of Oil and Gas Segment Cyber Security Standards*, November 2004. See http://www.naseo.org/eaguidelines/documents/cybersecurity/Comparison of Oil and Gas Security.pdf.

National Association of State Energy Officials (NASEO) and the National Associations of Regulatory Utility Commissioners (NARUC), *State Energy Assurance Guidelines* Version 3.1, December 2009. See http://www.naseo.org/energyassurance.

North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy (DOE) *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (June 2, 2010 The report examines three high-impact, low-frequency risks in detail: coordinated cyber, physical, or blended attacks; pandemic illness; and Geomagnetic Disturbances (GMD) and Electromagnetic Pulse (EMP) events. See http://www.nerc.com/news_pr.php?npr=587.

National Electric Reliability Corporation *Standard CIP-001-1 Sabotage Reporting*, January 2007. See http://www.naseo.org/eaguidelines/documents/cybersecurity/CIP standards.pdf.