The Evolution of the Smart Grid

The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of electronic intelligence capabilities for power control purposes and operations monitoring. The "Smart Grid" is the name given to this evolving intelligent electric power network. While these intelligent components may enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to "cyber" (i.e., computer-generated) attack, since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyber attack has increased focus on the cyber security of the Smart Grid.

Department of Energy's Vision for the Smart Grid

The U.S. Department of Energy (DOE) summarized its view of the potential of the Smart Grid by the year 2030 as "… a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between."

DOE's Smart Grid Investment Grant (SGIG) program received $3.5 billion from the American Recovery and Reinvestment Act of 2009. The program used the funds with the intent of stimulating the rapid deployment of advanced digital technologies needed to modernize the grid. According to a recent report from the DOE's Office of Inspector General (DOEIG), all the available grant funds from the SGIG program have been awarded to 99 recipients. An approach to cybersecurity was required as part of the SGIG application process. The DOEIG report observed that DOE approved these cybersecurity plans even though weaknesses in the plans were identified. The DOE responded to the report saying that it will require award recipients to update their cybersecurity plans later this year.

A Cybersecurity Roadmap for 2020

The DOE funded the development of the "Roadmap to Achieve Energy Delivery Systems Cybersecurity," (Roadmap) released in September 2011 by the Energy Sector Control System Working Group. This Roadmap provides a plan to improve the cybersecurity of the electricity, oil, and natural gas sectors. The Roadmap recognizes the changing landscape of cybersecurity, and the continuing need to seek out and address cybersecurity gaps and includes an implementation strategy for cybersecurity built on milestones to be achieved by the year 2020.

Current Status of DOE Smart Grid Efforts

The DOE has recently begun to update its vision for the Smart Grid, focusing on three key attributes it sees as desirable for the Smart Grid of the future. According to DOE, a reliable, secure, and resilient grid will be the key to achieving this vision.

Considerations for Congress

The very features which can add seamless integration and utility to the Smart Grid also add cyber vulnerabilities to electricity networks. Some assert that the Smart Grid and cybersecurity systems will have to develop along parallel but interconnected paths if the electric grid of the future is to develop in a manner that can enhance, and not impair, future economic development.

Testimony of Richard J. Campbell
Specialist in Energy Policy
Congressional Research Service

Before the Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
February 28, 2012

Good Morning Chairman, Ranking Member, and Members of the Subcommittee. My name is Richard Campbell. I am a Specialist in Energy Policy for the Congressional Research Service (CRS). On behalf of CRS, I would like to thank the Committee for inviting me to testify here today. My testimony will provide background on the development and cybersecurity of the Smart Grid, discussing the evolution of the Smart Grid, and planning for Smart Grid development and cybersecurity. I should note that CRS does not advocate policy or take a position on specific legislation.

The Evolution of the Smart Grid

The electrical grid in the United States comprises all of the power plants generating electricity, together with the transmission and distribution lines and systems which bring power to end-use customers. The "grid" also connects the many publicly and privately owned electric utility and power companies in different states and regions of the United States.[1]

[1] As of 2007, there were 210 investor-owned electric utilities, 2,009 publicly-owned electric utilities, 883 consumer-owned rural electric cooperatives, and nine federal electric utilities. Energy Information Administration (EIA), *Electric Power Industry Overview 2007*, http://www.eia.doe.gov/electricity/page/prim2/toc2.html.

However, with changes in federal law,[2] regulatory changes, and the aging of the electric power infrastructure as drivers, the grid is changing from a largely patchwork system built to serve the needs of individual electric utility companies to essentially a national interconnected system, accommodating massive transfers of electrical energy among regions of the United States.

The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of electronic intelligence capabilities for power control purposes and operations monitoring. The "Smart Grid" is the name given to this evolving intelligent electric power network.[3] While these intelligent components may enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to "cyber" (i.e., computer-generated) attack, since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyber attack has increased focus on the cyber security of the Smart Grid.

Department of Energy's Vision for the Smart Grid

Expectations vary of what a Smart Grid could accomplish, and the estimated costs of a system rise with the increased scope and attributes of a system. Some see the Smart Grid of the future as a system spanning the nation from coast to coast, able to seamlessly combine distributed

[2] Key legislation include the Public Utility Regulatory Policies Act of 1978, the Energy Policy Acts of 1992 and 2005, and the Energy Independence and Security Act of 2007.

[3] The Smart Grid is one of the options being discussed for the future of U.S. electricity networks and would build interactive intelligence into electricity transmission and distribution systems across the United States. Energy efficiency and energy conservation could be enhanced by demand-side management programs enabled by the wide scale deployment of smart meters. Energy storage projects could enhance such a system, providing options for peak load management and potentially allowing for even greater cost savings. See CRS Report R41493, *Options for a Federal Renewable Electricity Standard*, by Richard J. Campbell.

resources and central power stations across the three major interconnections[4] of the United States. Under such visions, distributed and renewable energy resources could be efficiently integrated into the grid, with power (for example) from intermittent wind generation channeled by sensors and intelligent electronics from multiple widely dispersed sites to where power is needed anywhere on the grid. The efficiency and economy of all grid operations could conceivably be optimized by similarly harnessing all power generation to take advantage of a wide range of generation and storage resources across the United States.[5]

The U.S. Department of Energy (DOE) summarized its view of the potential of the Smart Grid by the year 2030 as:

> … a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between.[6]

Federal funding has been provided to help develop concepts and technologies for the Smart Grid. The American Recovery and Reinvestment Act of 2009 (P.L.111-5) provided $4.5 billion in funding to DOE for projects to modernize the grid.[7] DOE's Smart Grid Investment Grant (SGIG) program[8] received $3.5 billion of these funds with the expressed purpose of stimulating the rapid deployment of advanced digital technologies needed to modernize the grid.[9]

---

[4] The Eastern, Western, and Texas interconnections of the U.S. grid. See http://www.eia.doe.gov/cneaf/electricity/chg_stru_update/fig7.html.

[5] CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[6] United States Department of Energy, Office of Electric Transmission and Distribution, *"GRID 2030" A NATIONAL VISION FOR ELECTRICITY'S SECOND 100 YEARS*, July 2003, p. 27, http://www.oe.energy.gov/DocumentsandMedia/Electric_Vision_Document.pdf.

[7] CRS Report R40412, *Energy Provisions in the American Recovery and Reinvestment Act of 2009 (P.L. 111-5)*, coordinated by Fred Sissine.

[8] The SGIG program was established by the Energy Independence and Security Act of 2007 (P.L. 110-140).

[9] See FEDCONNECT Opportunity: Recovery Act - Smart Grid Investment Grant Program, http://www.fedconnect.net/FedConnect/?doc=DE-FOA-0000058&agency=DOE.

The SGIG is a cost-shared program, meaning recipients of grants were to provide as much as 50% of a project's total costs. Topics for grants from the program focused on:

- Equipment Manufacturing.
- Customer Systems.
- Advanced Metering Infrastructure.
- Electric Distribution Systems.
- Electric Transmission Systems.
- Cross Cutting Systems.

According to a recent report[10] from the DOE's Office of Inspector General (DOEIG), all the available grant funds from the SGIG program have been awarded to 99 recipients, with awards ranging in value from $397,000 to $200 million. An approach to cybersecurity was required as part of the SGIG application process. Recipients of awards were required to submit a detailed cybersecurity plan addressing specific elements including threat detection, risk assessment, and risk mitigation.[11] The DOEIG report observed that DOE approved these cybersecurity plans even though weaknesses in the plans were identified and not fully addressed. The DOEIG was concerned that if these weaknesses are not properly addressed in the 3-year duration of the award, they could lead to cybersecurity gaps and subsequent compromises in system integrity.[12] The DOE responded to the report saying that it will require award recipients to update their cybersecurity plans later this year.[13]

---

[10] DOE Office of Inspector General, Office of Audits and Inspections, *The Department's Management of the Smart Grid Investment Grant Program*, OAS-RA-12-04, January 2012, http://energy.gov/sites/prod/files/OAS-RA-12-04.pdf.

[11] Ibid.

[12] Ibid.

[13] Ibid. See Appendix 3, Memorandum to DOEIG from DOE's Office of Electric Delivery and Energy Reliability.

A Cybersecurity Roadmap for 2020

The DOE funded the development of the "Roadmap to Achieve Energy Delivery Systems Cybersecurity,"[14] (Roadmap) released in September 2011 by the Energy Sector Control System Working Group. This Roadmap provides a plan to improve the cybersecurity of the electricity, oil, and natural gas sectors.

The Roadmap is an update of an earlier 2006 effort which established a "common vision" for industry and government to develop, deploy, and maintain control systems capable of surviving an intentional cyber attack without the loss of critical functions. The Roadmap recognizes the changing landscape of cybersecurity, and the continuing need to seek out and address cybersecurity gaps. Cyber threats to energy delivery systems are seen as real and becomingly increasingly innovative. The Roadmap recognizes that developing a culture of security that focuses on more than simple compliance with a list of requirements will be needed to achieve a resilient energy system. The Roadmap includes an implementation strategy for cybersecurity built on milestones to be achieved by the year 2020. The milestones focus on continual risk assessment, incident management, and sustained cybersecurity improvements.

[14] Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

Current Status of DOE Smart Grid Efforts

The DOE has recently begun to update its vision for the Smart Grid, focusing on three key attributes it sees as desirable for the Smart Grid of the future:[15]

- A seamless, cost-effective electricity system from generation to end use.
- A system capable of meeting clean energy demands and capacity requirements, accommodating all generation choices.
- A system which allows all consumers to participate and enables customer choice.

According to this updated vision, the Smart Grid will still see regional diversity in power choices, while allowing for the development of a national framework. The Smart Grid should also be able to accommodate new products and services. According to DOE, a reliable, secure, and resilient grid will be the key to achieving this vision.

Considerations for Congress

The very features which can add seamless integration and utility to the Smart Grid also add cyber vulnerabilities to electricity networks. Some assert that the Smart Grid and cybersecurity systems will have to develop along parallel but interconnected paths if the electric grid of the future is to develop in a manner that can enhance, and not impair, future economic development.

---

[15] U.S. Department of Energy, *Visioning the 21st Century Electricity Industry: Strategies and Outcomes for America*, February 2012, http://www.nationalelectricityforum.org/pdfs/DOE_vision_presentation.pdf.

Congress could provide funding for research and development of technologies and systems to bridge gaps in cybersecurity and build the Smart Grid. Federal funding could also be used to bring government and industry together in forums to address the needs and directions of these developing systems.

Congress may also provide for a regulatory framework which could achieve a basic level of cybersecurity. But due to the constantly changing nature of cyber threats, it is unlikely that effective cybersecurity of the grid will be achieved by regulation alone. Some assert that electric utilities must be focused on cybersecurity as keenly as they are on their current obligation to serve or to provide shareholder value.

Thank you again for the invitation to appear today. I will be pleased to address any questions you may have.