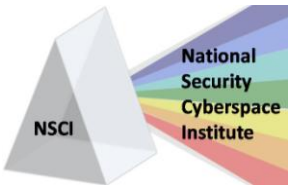

U.S. Smart Grid Security: How Are We Doing?

Kathryn Stephens, NSCI
October 19, 2011

What is the Smart Grid?

According to an NIST report, Smart Grids are "next-generation electrical grids that attempt to predict and intelligently respond to the behavior and actions of all electric power users connected to it – suppliers, consumers, and those that do both – in order to efficiently deliver reliable, economical and sustainable electricity services."[1] The Smart Grid would use networking and automation to control the flow and delivery of electricity to consumers and is made up of connected meters and sensors linking every home and business to power plants, wind farms, and fossil-fuel-powered generating plants.[2]

The Smart Grid was first established in the Energy Independence and Security Act of 2007, and the U.S. government designated $4.5 billion for Smart Grid development in the American Recovery and Reinvestment Act (ARRA) in 2009. Cost estimates for smart grid development vary significantly, ranging from $100 billion to $400 billion over the next decade.[3] The Electric Power Research Institute (EPRI) released a report in March 2011 that estimates the total cost of a national smart grid to be between $338 billion and $476 billion over the next twenty years.[4] This new report is an update to the previous EPRI smart grid cost estimate from 2004, which predicted the total cost to be $165 billion.[5] The $4.5 billion federal government investment from the ARRA accounts for less than five percent of the total cost in even the most modest cost estimate. We have not seen any details on how the government plans to fund the remaining 95% of implementing Smart Grid.

In order to connect homes and businesses to the Smart Grid, electric meters will be replaced with smart meters, which would give home and business owners access to energy prices and changes in prices, so that consumers could run electrical equipment when the rates are lowest. The Federal Government plans to distribute more than 40 million smart meters in homes and businesses, 200,000 smart transformers, 850 sensors, and 700 automated substations, in addition to industry contributions.[6]

Numerous individuals and organizations have questioned various aspects of Smart Grid implementation, including how and who will fund the remaining 95% of the investment required, the resulting ability of government to monitor and control electricity consumption, privacy implications and cyber security risks.

Why are we developing the Smart Grid?

The current U.S. electricity grid is highly fragmented, and 80 percent of the grid is owned and operated by private companies.[7] According to the U.S. government, the Smart Grid is expected to provide a fully interoperable, standardized network for power distribution.

---

[1] *U.S., Europe Collaborating on Smart Grid Standards Development.* (2011, September 15). Retrieved from Homeland Security News Wire: http://www.homelandsecuritynewswire.com/us-europe-collaborating-smart-grid-standards-development
[2] Jackson, W. (2010, October 13). *First set of Smart Grid standards submitted to energy regulators.* Retrieved from Federal Computer Week: http://fcw.com/articles/2010/10/13/smart-grid-standards.aspx
[3] *Sticker Shock: EPRI Says Smart Grid Will Cost $165 Billion Over 20 Years.* (2010, February 15). Retrieved from Smart Grid News: http://www.smartgridnews.com/artman/publish/Business_Policy_Regulation/Sticker-Shock-EPRI-Says-Smart-Grid-Will-Cost-165-Billion-Over-20-Years-1882.html
[4] Electric Power Research Institute. (2011, March). *Estimating the Costs and Benefits of the Smart Grid.* Retrieved from http://ipu.msu.edu/programs/MIGrid2011/presentations/pdfs/Reference%20Material%20-%20Estimating%20the%20Costs%20and%20Benefits%20of%20the%20Smart%20Grid.pdf
[5] *EPRI does the math on total smart grid cost (and it's a lot).* (2011, April 7). Retrieved from Smart Grid Newsl: http://www.smartgridnews.com/artman/publish/news/EPRI-does-the-math-on-total-smart-grid-cost-and-it-s-a-lot-3604.html
[6] Caruso, J. (2010, August 17). *What is the 'Smart Grid'?.* Retrieved from Network World: http://www.networkworld.com/newsletters/lans/2010/081710-smart-grid.html
[7] Marsan, C. D. (2009, October 29). *Q&A: Why IP is the right choice for Smart Grid* . Retrieved from Network World: http://www.networkworld.com/news/2009/102909-smart-grid-ipv6-qa.html

Kathryn Stephens, NSCI
October 19, 2011

The Smart Grid will allow utilities *(and potentially others, such as the government)* to communicate with consumers to monitor power and help consumers reduce their power usage. In addition to the reduction of power usage and cost savings to consumers, Smart Grid development could also help spur innovation and could impact the economy because of the required development and production.[8] Development of the Smart Grid program was one element of President Obama's economic recovery program because of its potential to create jobs while contributing to energy independence and a reduction in carbon emissions.[9]

The Smart Grid program aims to increase energy efficiency, reliability and security, and to allow the transition to renewable sources of energy. Smart Grids will also "ease the incorporation of renewable energy sources, energy saving devices, and electric vehicles into the power system."[10]

Annabelle Lee, the Senior Cyber Security Strategist at the National Institute of Standards and Technology, says the Smart Grid is necessary for the nation to end its dependence on foreign oil, and to increase electricity capacity for new technologies such as electric vehicles.[11]

Because the Smart Grid would ultimately rely on the Internet and wireless connections to work, malicious hackers could find vulnerabilities to exploit to gain access to the grid.

Cyber Risks to the Smart Grid

According to the Project Grey Goose Report on Critical Infrastructure released in February 2010, attacks against the power grid are likely to rise and intensify due to the increasing focus and investment into Smart Grid research and pilot projects. Jeffrey Carr, Project Grey Goose principal investigator, says there have already been "at least 120 instances" of successful power grid attacks dating back to 2001.[12]

There are several cyber risks to Smart Grid security. One issue is each device connected to the Smart Grid is then a potential target for hackers. Smart switches will also be needed, and will need to be more rugged than switches typically used in homes and office.[13] Mike Davis, a senior security consultant for IOActive, says the new smart meters already being deployed contain "buggy software that's easily hacked." According to Davis, the smart meters use no encryption and do not ask for authentication before running software updates.[14]

The Smart Grid's distribution and connectivity exposes networks and systems that have historically relied on isolation for security. The two-way communication between customers and utility companies could give hackers a way into the Smart Grid network, which could allow a hacker to gain control of the power supply to a single home, a neighborhood, or a much broader area. Kenneth Van Meter, Lockheed Martin's general manager of Energy and Cyber Services, says that each of the 440 smart meters that will

---

[8] *Locke: Government 'Moving Fast' on Smart-Grid Technology.* (2010, October 18). Retrieved from The Daily Beast: http://www.thedailybeast.com/newsweek/blogs/the-gaggle/2010/10/18/locke-goverment-moving-fast-on-smart-grid-technology.html
[9] Jackson, W. (2010, October 13). *First set of Smart Grid standards submitted to energy regulators.* Retrieved from Federal Computer Week: http://fcw.com/articles/2010/10/13/smart-grid-standards.aspx
[10] *U.S., Europe Collaborating on Smart Grid Standards Development.* (2011, September 15). Retrieved from Homeland Security News Wire: http://www.homelandsecuritynewswire.com/us-europe-collaborating-smart-grid-standards-development
[11] *Is the Smart Grid Really Going to Happen?* (2009, September 24). Retrieved from Federal News Radio: http://www.federalnewsradio.com/?nid=656&sid=1770238
[12] Higgins, K. J. (2010, February 19). *Spike In Power Grid Attacks Likely In Next 12 Months.* Retrieved from Dark Reading: http://www.darkreading.com/security/vulnerabilities/223000369/spike-in-power-grid-attacks-likely-in-next-12-months.html
[13] Caruso, J. (2010, August 17). *What is the 'Smart Grid'?.* Retrieved from Network World: http://www.networkworld.com/newsletters/lans/2010/081710-smart-grid.html
[14] Goodin, D. (2009, June 12). *Buggy 'smart meters' open door to power-grid botnet.* Retrieved from The Register: http://www.theregister.co.uk/2009/06/12/smart_grid_security_risks/

be connected to the grid by 2015 are new "hackable points." "If you can communicate with it, you can hack it," says Van Meter.[15] While the networked environment the Smart Grid offers is essential to realizing its full benefits, the connectivity also adds complexity, interdependencies and vulnerabilities to the grid.

If a hacker is able to gain access, devices could be tricked into requesting more power than is actually needed and overburdening the grid. Alternatively, devices could be made to request less power than is actually needed, which could result in widespread "brown-outs." The Smart Grid would almost certainly be a target for terrorists, who may try to disrupt power distribution in order to undermine confidence in the utility industry, or destabilize the population.

Because of the vulnerabilities introduced by networking smart devices to create the Smart Grid, and because of the lack of a single oversight authority, there is the potential for fraud, denial of power, and privacy breaches. The mix of different technologies and utility systems presents additional issues and vulnerabilities in implementation. Not only will the Smart Grid be vulnerable to attacks from cyber criminals and hackers, but the power supply could also be compromised by buggy software, user errors, and equipment failures. In addition, Smart Grid security will be, in part, a responsibility of the home or business owner, who will be accountable for their usage of smart appliances and devices.[16]

Privacy Concerns

Smart meters will also collect more information than traditional power meters, potentially including personally identifiable information that could be used by cyber criminals for identity theft and fraud.[17]

According to a report from the Ontario Information and Privacy Commissioner and the Future of Privacy Forum (FPF), smart meters could reveal personal information that should not be monitored. For example, utility companies will be able to monitor whether a house has an alarm system and how often it is activated, or when occupants usually shower. The transition to the Smart Grid will result in the collection of more data than ever before, which may be vulnerable given the lack of solid data retention policies that govern the use of personally identifiable information in the utility industry.[18] There must be clear policies for how this information would be compiled and used by utility companies.

In August 2011, the California Public Utilities Company (CPUC) adopted privacy rules for smart meters to protect consumers from cyber intrusions. CPUC's decision made California the first state to establish a framework for protecting consumer privacy, despite the fact that Smart Grid development has been underway since 2007.[19]

There are also several legal issues that must be considered. If the grid is attacked, certain responses to the attack would be illegal, even if hackers or cyber criminals caused damage or disrupted access to the grid. No government agency can give the private sector immediate help if they are attacked, and reporting

[15] Storm, D. (2010, October 7). *440 million new hackable smart grid points.* Retrieved from Computer World: http://blogs.computerworld.com/17120/400_million_new_hackable_smart_grid_points
[16] *Smart Grids and Security (Intro).* (2009, August 19). Retrieved from Securosis: http://securosis.com/blog/smart-grids-and-security-intro/
[17] Krebs, B. (2009, November 18). *Experts: Smart grid poses privacy risks.* Retrieved from Washington Post: http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html
[18] Krebs, B. (2009, November 18). *Experts: Smart grid poses privacy risks.* Retrieved from Washington Post: http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html
[19] *California Adopts First Cybersecurity Plan for Household Energy Meters.* (2011, August 5). Retrieved from The New New Internet: http://www.thenewnewinternet.com/2011/08/05/california-adopts-first-cybersecurity-plan-for-household-energy-meters/

an intrusion would only launch an investigation, not permission to defend the grid. Intrusions into the grid could also come from foreign actors or governments, further complicating mitigation or defense.[20]

Has the grid been hacked before?

Some report the grid has already been compromised. An article in the Wall Street Journal from April 2009 claimed both China and Russia have already compromised the power grid, leaving malicious code behind that could disrupt or destroy portions of the grid if activated.[21] Intelligence officials claim the intruders were attempting to map U.S. infrastructure, including the electrical grid and other infrastructure systems. Former Director of National Intelligence Dennis Blair said China and Russia could disrupt the U.S. information infrastructure using the software left behind.[22]

U.S. adversaries are already aware of vulnerabilities and access points to the power grid. A 2009 report from Jian-Wei Wang, a network analyst from China's Dalian University of Technology, modeled how the West Coast power grid is connected and demonstrated how an outage on one subnetwork would affect adjacent networks. The report identified weaknesses of the West Coast grid, and discussed cascading failures, which is an outage that triggers failures across entire networks.[23] The massive blackouts in 2003 that affected 50 million people were reportedly caused by PLA actors that gained access to the power grid and set off cascading failures.[24]

Mike Davis, a security consultant for IOActive, created and demonstrated a piece of software in 2009 that spreads automatically between smart grid hardware in different homes, and is capable of shutting down grid equipment. IOActive claimed an attacker with simple equipment could take control of the Smart Grid, "allowing for the en masse manipulation of service to homes and businesses."[25]

International Cooperation

According to U.S. Secretary of Commerce Gary Locke, European nations such as Germany and France are currently "working aggressively on Smart Grids." Locke also points out each country is creating its own standards for the Smart Grid, so Smart Grid systems may not be compatible internationally.[26]

The UK's SmartReach consortium is calling for the UK government to create a single, long-range radio network separate from existing networks and classified as critical national infrastructure to connect new smart meters for gas and electricity. The plan suggests linking all the meters to a central or regional processing center, and using a single network in order to cut costs from multiple service providers as well

---

[20] Zhang, Z. (2011, August). *Cohesive Cybersecurity Policy Needed For Electric Grid .* Retrieved from National Defense: http://www.nationaldefensemagazine.org/archive/2011/August/Pages/CohesiveCybersecurityPolicyNeededForElectricGrid.aspx
[21] Coleman, K. (2010, June 17). *Protecting the SMART Grid From Cyber Attack.* Retrieved from Defense Tech: http://defensetech.org/2010/06/17/protecting-the-smart-grid-from-cyber-attack/
[22] Gorman, S. (2009, April 8). *Electricity Grid in U.S. Penetrated By Spies.* Retrieved from Wall Street Journal: http://online.wsj.com/article/SB123914805204099085.html
[23] Vijayan, J. (2009, September 14). *DHS to review report on vulnerability in West Coast power grid.* Retrieved from Computer World: http://www.computerworld.com/s/article/9138017/DHS_to_review_report_on_vulnerability_in_West_Coast_power_grid
[24] Sorkin, J. (2009, March 23). *Security researchers: Smart Grid is vulnerable to attacks .* Retrieved from Top News: http://topnews.us/content/24527-security-researchers-smart-grid-vulnerable-attacks
[25] Slocum, Z. (2009, March 24). *Report: Smart-grid hackers could cause blackouts.* Retrieved from CNet: http://news.cnet.com/8301-1009_3-10201651-83.html
[26] *Locke: Government 'Moving Fast' on Smart-Grid Technology.* (2010, October 18). Retrieved from The Daily Beast: http://www.thedailybeast.com/newsweek/blogs/the-gaggle/2010/10/18/locke-goverment-moving-fast-on-smart-grid-technology.html

as to reduce system integration issues. SmartReach is also calling for security to be built into Smart Grid applications, since detailed customer information could be a target for hackers and criminals.[27]

The U.S. Commerce Department's NIST and the European Union's (EU) Smart Grid Coordination Group (SG-CG) recently announced they would work together to develop Smart Grid standards aimed at helping spur innovation in the electrical sector and facilitate interoperability between international grids. NIST and SG-CG will share information on: legislation and regulations; work methods and time lines; testing and certification frameworks; and cybersecurity requirements and technologies.[28] NIST and the EU are working to create an interoperable international grid, which would allow devices and networks from Europe to work seamlessly on the U.S. grid. While the grids would not routinely interconnect, manufacturers are hoping to produce equipment that could be used on smart girds around the world.[29] It would seem this may increase the threat for attacks on smart meters and other grid access points.

What is being done?

Current protection efforts aimed at electric infrastructure are split between several groups and are addressed in several laws and regulatory reports.

The 2007 Energy Independence and Security Act (EISA) divided responsibility for developing Smart Grid security. The Energy Department was given responsibility for developing and implementing the Smart Grid, NIST was tasked with establishing development standards, and the Federal Energy Regulatory Commission (FERC) enforces standards for the nation's power plants. Other agencies, including the Defense and Interior Departments, the Environmental Protection Agency, and the Federal Communications Commission, are also involved in Smart Grid development and implementation.[30]

Following the release of EISA, FERC began to develop an initial set of interoperability and cyber standards, but has not yet found a coordinated way to monitor how industry is following the standards. EISA gave FERC the authority to adopt standards, but failed to provide specific enforcement authority for FERC. According to the GAO, this means the standards will remain voluntary until regulators are given oversight abilities or other authorities to enforce them.[31] EISA also allows utilities to self-identify what they determine to be critical cyber assets. Only those assets that are defined as critical are subject to critical infrastructure protection standards from FERC. [32] NERC has reported that many utilities underreport their critical cyber assets in order to avoid compliance requirements.[33]

NIST released its Guidelines for Smart Grid Cyber Security in September 2010, which included 189 high-level security requirements. The Guidelines included information on security requirements, a framework for assessing risks, evaluation of privacy issues at personal residences, and strategies for businesses to

---

[27] Grant, I. (2010, October 21). *Smart meters need single network, say BT partners.* Retrieved from Computer Weekly: http://www.computerweekly.com/Articles/2010/10/21/243476/Smart-meters-need-single-network-say-BT-partners.htm
[28] *U.S., Europe Collaborating on Smart Grid Standards Development.* (2011, September 15). Retrieved from Homeland Security News Wire: http://www.homelandsecuritynewswire.com/us-europe-collaborating-smart-grid-standards-development
[29] Jackson, W. (2011, September 14). *NIST, Europeans to collaborate on smart-grid standards.* Retrieved from Government Computer News: http://gcn.com/articles/2011/09/14/smart-grid-cooperation-nist-eu.aspx
[30] Aitoro, J. R. (2010, January 1). *NIST releases update to smart grid standards.* Retrieved from Nextgov: http://www.nextgov.com/nextgov/ng_20100120_4191.php
[31] GAO. (2011, January). *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed.* Retrieved from U.S. Government Accountability Office: http://www.gao.gov/new.items/d11117.pdf
[32] Campbell, R. J. (2011, June 15). *The Smart Grid and Cybersecurity - Regulatory Policy and Issues.* Retrieved from Congressional Research Service: http://www.fas.org/sgp/crs/misc/R41886.pdf
[33] Flick, T. (2009). *Hacking the Smart Grid.* Retrieved from Blackhat.com: http://www.blackhat.com/presentations/bh-usa-09/FLICK/BHUSA09-Flick-HackingSmartGrid-PAPER.pdf

protect the power grid.[34] The guidelines fail to address the potential vulnerabilities that can occur when different vendors have to integrate products. Michael Assante, president and chief executive officer of the National Board of Information Security Examiners, calls the guidelines a "good starting point," but says "we need key design principles to promote security in holistic solutions."[35]

NIST has also started a Smart Grid Cyber Security Coordination Task Group (CSCTG) which includes volunteers from the public and private sectors, academia, regulatory organizations and federal agencies. The NIST Interagency Report (NISTIR) 7628, *Smart Grid Cyber Security Strategy and Requirements,* is the culmination of the group's findings on grid vulnerabilities, vulnerability classes, and security requirements for the Smart Grid. The report is expected to serve as the foundation for standards developed by NIST and the Smart Grid Interoperability Panel (SGIP).[36] While the paper adequately addresses many concerns and vulnerabilities associated with the Smart Grid, it fails to provide any answers or suggestions for mitigating the threats.

The U.S. Department of Energy has also started a Smart Grid stimulus program, which is expected to spur investment in Smart Grid security efforts. The Smart Grid Cyber Security Report from Pike Research claims that utility companies will invest $21 billion in grid security by 2015. According to the report, security investment will be distributed in five areas: policy, planning and awareness; equipment protection and configuration management; monitoring and incidence response; access, audit, and integrity; and risk management.[37] Recent standard initiatives from NIST and the Smart Grid objectives being promoted by the Federal Energy Regulatory Commission are also expected to spur investment.

GAO has identified six key challenges to Smart Grid security: the regulatory environment makes it difficult to ensure cybersecurity; utilities focus too heavily on compliance instead of comprehensive security; the lack of an effective information sharing mechanism; the lack of consumer education about the benefits, costs and risks with Smart Grid systems; the lack of security features built in to systems; and the electricity industry's need for metrics to evaluate cybersecurity.[38] The 2011 GAO report, "Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed," found major gaps in the NIST smart grid cybersecurity guidelines, and states that FERC has failed to develop a coordinated approach to overseeing standard implementation.[39]

What needs to be done?

Several things must be done in order to better secure the Smart Grid. Developers of smart meters and other grid devices must build security into devices in order to avoid firmware vulnerabilities that cannot be easily fixed later. There must also be more emphasis placed on designing a Smart Grid resilient to attacks that will inevitably occur. We must also define what the appropriate response is to an attack on the Smart

---

[34] *NIST Finalizes Initial Set Of Smart Grid Cyber Security Guidelines.* (2010, September 16). Retrieved from Space War: http://www.spacewar.com/reports/NIST_Finalizes_Initial_Set_Of_Smart_Grid_Cyber_Security_Guidelines_999.html
[35] Aitoro, J. R. (2010, September 7). *NIST releases cybersecurity guidelines for smart grid.* Retrieved from Nextgov: http://www.nextgov.com/nextgov/ng_20100907_6414.php
[36] NIST. (2010, January). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* Retrieved from National Institute of Standards and Technology: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf
[37] Collins, H. (2010, February 9). *FedsWill Spur Smart Grid Cyber-Security Investment Growth to $21 Billion by 2015, Report Claims* . Retrieved from Government Technology: http://www.govtech.com/security/Feds-Will-Spur-Smart-Grid-Cyber-Security.html
[38] GAO. (2011, January). *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed.* Retrieved from U.S. Government Accountability Office: http://www.gao.gov/new.items/d11117.pdf
[39] Maize, K., & Patel, S. (2011, March 1). *Do Smart Grid Standards Adequately Address Security Problems?* Retrieved from Managing Power: http://www.managingpowermag.com/smart_grid/Do-Smart-Grid-Standards-Adequately-Address-Security-Problems_305.html

Grid ranging from employee mistakes and equipment malfunctions, to Internet viruses and coordinated attacks from a state or terrorist group. The government must provide industry with clear, cohesive standards and policies. "There is no shortage of government policies for protecting critical infrastructure sectors from network vulnerabilities. What is missing is a focused comprehensive cybersecurity policy for the electricity sector."[40]

Current NERC information sharing and reliability standards are valuable, but do not provide a single Smart Grid security policy. In addition, the following standards are relevant to the Smart Grid: IEEE 1686-2007, *IEEE Standard for Substation Intelligence Electronic Devices (IEDs) Cyber Security Capabilities; Security Profile for Advanced Metering Infrastructure,* v1.0, Advanced Security Acceleration Project – Smart Grid; *UtilityAMI Home Area Network System Requirements Specification;* and IEC 62351 1-8, Power System Control and Associated Communications – Data and Communication Security.[41] These standards may address one part, or a small piece of Smart Grid security, but do not provide a unified policy for developing Smart Grid security.

A comprehensive Smart Grid security policy is absolutely necessary and should address: information sharing; the role of industry in Smart Grid security; how to respond to cyber attacks; awareness of legal implications that address attacks on critical infrastructure; an evaluation of foreign systems; and government development and security funding.

Security will rely largely on industry's ability and willingness to share information. Exchanging data through the traditional channel, the Electricity Sector Information Sharing and Analysis Center, can be difficult since the ISAC is owned by the North American Electric Reliability Corp., an international regulatory authority. Utility companies should have a better way to communicate threat and vulnerability information in order to improve security for the entire grid.[42]

It seems government is pushing harder than industry in developing and implementing the Smart Grid, which may be dangerous if security is not a priority. Security consultant Tony Flick says Smart Grid development has become a "gold rush" to get government money, but when industry rushes new technologies to market, they are more likely to be flawed and vulnerable.[43] Because utilities are only eligible for smart-grid money from Obama's stimulus package if they meet aggressive deadlines, security has taken a backseat to production and implementation. U.S. Secretary of Commerce Gary Locke says the federal government is moving aggressively on Smart Grid development in order to spur new technologies and innovation in the United States.[44] This aggressive government spending absent a cohesive development plan has led to several disjointed Smart Grid software versions.

Patricia Titus, chief information security officer for Unisys Federal Systems and former CISO for the TSA, says the utility industry needs to "take a breath" and "determine whether adopting Smart Grid technology

---

[40] Zhang, Z. (2011, August). *Cohesive Cybersecurity Policy Needed For Electric Grid .* Retrieved from National Defense: http://www.nationaldefensemagazine.org/archive/2011/August/Pages/CohesiveCybersecurityPolicyNeededForElectricGrid.aspx
[41] NIST. (2010, January). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* Retrieved from National Institute of Standards and Technology: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf
[42] Jackson, W. (2009, September 24). *Sharing threat data is key to securing the power grid.* Retrieved from Government Computer News: http://gcn.com/articles/2009/09/28/gcn-interview-seth-bromberger-power-grid-security.aspx
[43] Robertson, J. (2009, July 31). *Security experts offer caution on smart grids .* Retrieved from MSNBC: http://www.msnbc.msn.com/id/32238717/ns/technology_and_science-security/t/security-experts-offer-caution-smart-grids/
[44] *Locke: Government 'Moving Fast' on Smart-Grid Technology.* (2010, October 18). Retrieved from The Daily Beast: http://www.thedailybeast.com/newsweek/blogs/the-gaggle/2010/10/18/locke-goverment-moving-fast-on-smart-grid-technology.html

will exacerbate or solve problems."[45] Given the lack of industry standards for security, reliability, data sharing, and privacy, the government may well be wasting its money on technologies that are not interoperable, and increase critical infrastructure vulnerability to attacks.

[45] Higgins, K. J. (2010, February 19). *Spike In Power Grid Attacks Likely In Next 12 Months.* Retrieved from Dark Reading: http://www.darkreading.com/security/vulnerabilities/223000369/index.html