ASA

Annie Searle & Associates LLC

Research Note

Not So Smart: Smart Grid and Cybersecurity Challenges of the Department of Energy

By Brooke R. Brisbois

Applicable Sectors: energy, defense
Keywords: Department of Energy, smart grid, cybersecurity
Abstract: Explores the challenges faced by the Department of Energy with regard to smart grid technology and cybersecurity. In particular, discusses policy issues surrounding these problems.

The Department of Energy (DOE) plays a pivotal role in the critical infrastructure of the U.S. It is charged with not only the regulation and generation of the nation's power supply, but the protection of the energy infrastructure as well. Before the rise of the personal computer, Internet, and general digital age, the DOE's focus was on nuclear energy, nuclear attack, and the Cold War. Today, remnants of that era still linger on the DOE's website: the "About Us" page states that they are "working to ensure America's Energy Future, Scientific & Technological Leadership, Nuclear Security and to resolve the environmental legacy of the cold war."[1] Curiously absent from this statement is any mention of cybersecurity or cyberattack. This is remarkable because cybersecurity is arguably the DOE's number one concern, due to the vulnerability of legacy industrial control systems, the widespread implementation of smart grids, and poorly managed cybersecurity practices.

Before the DOE's concerns can be addressed, however, a clear picture of the department itself must be given. As stated on its website, part of the DOE's mission is to "ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges."[2] This mission statement gives a tall order; the department is essentially expected to guarantee America's security and prosperity with regard to any issues in the energy sector. Moreover, the mission statement does not address *how* the department should be doing any of these things, except through "transformative science and technology solutions."[3]

To further demonstrate the sheer size and criticality of their mission, a clearer view of the energy sector landscape in the U.S. must be given. Begin by considering how many types of energy the U.S. is involved with. Oil, natural gas, and electricity are a few. Now delve deeper into one of those areas–try the electric utility sector. According to *Electricity Regulation in the U.S.: A Guide,* the U.S. electric industry "comprises over 3,000 public, private, and cooperative utilities, more than 1,000 independent power generators, three regional synchronized power grids, eight electric reliability councils, about 150 control-area operators, and thousands of separate engineering, economic, environmental, and land-use regulatory authorities."[4] In addition to the variety of different organizations within the industry, there is variety of

another kind: industrial control systems, old and new, some state-of-the-art and others woefully old, all needed to monitor the flow of electricity through about 211,000 miles of transmission lines in the U.S.[5] Within these industrial control systems lie the two interconnected problems that currently plague the DOE: smart grids and cybersecurity.

In 2009, the American Recovery and Reinvestment Act was created in order to encourage economic growth. Spurred by this incentive, the DOE invested more than $31 billion toward clean energy projects throughout the U.S., many of which were smart grid-related projects.[6] As explained on the government's Smart Grid website, a smart grid is an electric grid, consisting of not only the technology that has existed since the 1890s (such as transmission lines, substations, and transformers), but the technology of today as well (such as computers, sensors, and automation).[7] Updating legacy systems to include smart grids is a necessity in the digital age; yet doing so brings a host of new problems. Brian Smith of *Smart Grid News* illuminates these issues, explaining, "The challenge with cybersecurity and smart grid is that there is no finish line…not one that remains constant throughout the life of the system being protected. Adversaries and threats evolve constantly and new vulnerabilities can be discovered at anytime."[8] This brand-new technology is ever changing, and so are the cybersecurity threats.

Smart grids are only a part of the DOE's cybersecurity problem. A majority of the 256 incidents that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to in 2013 were detected in organizations within the energy sector, some smart grid attacks and others not.[9] Incidents like these are a growing concern within the energy sector due to cyberattacks becoming more sophisticated in nature, as well as originating from increasingly organized (and militarized) sources. In a statement to the Senate Committee on Armed Services, General Keith B. Alexander advocated the importance of cybersecurity, explaining that the energy sector and other elements of critical infrastructure are specifically being targeted by foreign nation-states.[10] *Aljazeera America* reporter Michael Pizzi described the biggest fear associated with cybersecurity as one in which "enemy hackers…could infiltrate the U.S. power grid, shutting down government agencies, crashing planes into buildings, and grinding the economy to a halt."[11] Though nothing of this sort has happened *yet*, Pizzi highlights the opinion of security experts, who say a "large-scale attack on the U.S. power grid that could inflict mass casualties is within the realm of possibility."[12]

The DOE is not only facing challenges due to the mere presence of these threats and vulnerabilities, but also because of the way they are handling them. Though there are numerous standards, documents, and guidelines about smart grids and cybersecurity, there is no single, unifying standard for responding to these challenges. For example, a company that provides electric utilities can look to the National Institute of Standards and Technology (NIST) for cybersecurity guidelines, ICS-CERT or any private cybersecurity vendor for recommendations, the Federal Energy Regulatory Commission (FERC) for regulations, and the Department of Homeland Security (DHS), ICS-CERT, or any number of local or regional organizations for help with attacks. This complex mix of guidelines, agencies, and regulations cannot even be found in one place; the "Standards and Interoperability" section on the government Smart Grid website only mentions NIST, while the DOE's Cybersecurity Risk Management Process site page also mentions NIST as well as the North American Electric Reliability Corporation (NERC) critical infrastructure cybersecurity standards.[13] Any kind of escalation procedure or need to report and incident

to DHS or ICS-CERT is not explicitly mentioned on the DOE's website.[14]

The absence of clear guidelines, explicit communication channels, and a unified incident response procedure makes the issues of cyberattack and cybersecurity an almost insurmountable problem for the DOE. In order to address these issues, an unambiguous plan for cybersecurity must be implemented. The DOE currently has two documents that attempt to do this: the aforementioned *Electricity Subsector Cybersecurity Risk Management Process* and the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. The issue with both of these documents is that they lack specificity. The first is a risk management framework, and as such is intended to scale to the size of the organization that is implementing it.[15] It is quite coy about mandating actual cybersecurity requirements, and instead only tells the organization how to *determine* its requirements. Conversely, the *Roadmap* has clear goals and milestones with regard to cybersecurity, but again lacks well-defined actions to be executed in order to achieve those goals.

Perhaps to address this lack of clarity, President Obama issued two documents in 2013 that addressed the issue of cybersecurity in critical infrastructure in the U.S., with particular regard to communications and incident reporting. The first document is an executive order entitled "Improving Critical Infrastructure Cybersecurity" and the other is a Presidential Policy Directive/PDD-21 on the subject of "Critical Infrastructure Security and Resilience." Both address the challenges brought forth previously: the need for more coordinated efforts in cybersecurity across critical infrastructure entities. However, neither of these documents are mentioned in the "Cybersecurity Risk Management Process" on the DOE's website.

Additionally, these executive directives read much like the NIST framework; there are orders addressed to specific departments (i.e., DHS, etc.), but these are rather vague statements that qualify *what* but not *how*. For example, the Presidential Policy Directive states, under Strategic Imperative 1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience:

> As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.[16]

This section outlines what needs to be done (create two national critical infrastructure centers) and what they will do, but does not give any specific direction as to what an "integration and analysis function" that is needed would actually look like.[17] The executive order reads similarly, stating that the Secretary, Attorney General, and Director of National Intelligence should together establish a process that disseminates cybersecurity reports produced.[18] There is no mention of what *kind* of "cyber threat information" should be reported in this process, just that it should be reported.[19] It is also notable that in the Definitions sections of both documents "cybersecurity," "cyberattack," or "cyberwar" are nowhere to

be found. Though these presidential directives do give more direction than previous documents on the subject, there is still a substantial lack of the explicit guidance that is much needed in this sector. A recommendation to the DOE would be to clearly define cybersecurity, and cyberattacks and cyberwarfare in particular. It is of the utmost importance that any organization in the energy sector, regardless of its size, know what constitutes a critical cyberattack or an act of cyberwarfare, and when these incidences should be escalated and to whom.

In addition to better cybersecurity and smart grid guidelines, the energy sector needs more personnel versed in cybersecurity. While there are incentive programs, such as the National Science Foundation's CyberCorps, which offers to finance education in return for government service, the numbers are not growing to meet the need fast enough.[20] *Businessweek* writer Dune Lawrence discovered that while there is a big industry demand for cybersecurity, the wages do not typically reflect this, especially in government, where the need for new "cyberwarriors" is arguably the most critical.[21] It is becoming commonplace for government to lose talented cyberprofessionals to government contractors and private companies that can afford to pay more.[22]

However, this problem could be mitigated if government worked more closely with contractors and private companies on a strategically unified cybersecurity plan. This idea is not new to the department, and is specified in the *Roadmap* as a long-term milestone: In eight to ten years, there should be a "significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry."[23] In the same period, the DOE also expects that "private sector investment will surpass Federal investment in developing cybersecurity solutions for energy delivery systems."[24] These two goals can be met if government scholarship programs are changed. Instead of allowing students to work only for government entities, the scholarship should allow students to work for any cybersecurity position within the U.S. energy sector. Scholarships such as these would attract more people to the field through the prospect of the high income that is expected from government contractors and private companies.[25]

The DOE is one of the most critical departments in the U.S., but it also faces some of the most critical challenges, most notably those linked to the country's move into the digital age. Smart grids and cybersecurity are not only pressing issues now, but will continue to be for years to come. If the DOE can improve its incident response and communication strategies, as well as increase cybersecurity manpower, the risks to the nation's critical infrastructure can be significantly reduced, both now and in the future.

---

[1] "About Us." U.S. Department of Energy. n.d. Accessed Apr. 2014 <www.energy.gov>.

[2] Ibid.

[3] Ibid.

[4] *Electricity Regulation in the US: A Guide*. RAP Online. Mar. 2011. Accessed Apr. 2014 <www.raponline.org>.

[5] *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Energy Sector Control Systems Working Group. Sep.2011. Accessed Apr. 2014 <www.energy.gov>

[6] Ibid.

[7] "What is the Smart Grid?" U.S. Department of Energy. n.d. Accessed Apr. 2014 <www.smartgrid.gov>.

[8] Smith, Brian. "The 3 kinds of Cybersecurity Every Utility Needs (And A Reference Architecture You Need To Know About)." SmartGridNews.com. 27 Mar. 2014. Accessed Apr. 2014 <www.smartgridnews.com>.

[9] *ICS-CERT Monitor*. U.S. Department of Homeland Security. Oct-Dec. 2013. Accessed Apr. 2014 <ics-cert.us-cert.gov>.

[10] "Statement of General Keith B. Alexander Commander U.S. Cyber Command Before the Senate Committee on Armed Services." U.S. Department of Defense. 12 Mar. 2013. Accessed Apr. 2014 <www.defense.gov>.

[11] Pizzi, Michael. "Cyberwarfare Greater Threat to U.S. Than Terrorism, Say Security Experts." *Aljazeera America.* Al Jazeera America, LLC. 7 Jan. 2014. Accessed Apr. 2014 <www.america.aljazeera.com>.

[12] Ibid.

[13] "Standards and Interoperability" U.S. Department of Energy. n.d. Accessed Apr. 2014 <www.smartgrid.gov>.

[14] "Cybersecurity Risk Management Process." U.S. Department of Energy. n.d. Accessed Apr. 2014 <www.energy.gov>.

[15] *Electricity Subsector Cybersecurity Risk Management Process*. U.S. Department of Energy. May 2012. Accessed Apr. 2014 <www.energy.gov>.

[16] Obama, Barak. "Presidential Policy Directive - Critical Infrastructure Security and Resilience." White House. 12 Feb. 2013. Accessed Apr. 2014 <www.whitehouse.gov>.

[17] Ibid.

[18] Obama, Barak. "Executive Order: Improving Critical Infrastructure Cybersecurity." White House. 12 Feb. 2013. Accessed Apr. 2014 <www.whitehouse.gov>.

[19] Ibid.

[20] Lawrence, Dune. "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016." *Businessweek.* 15 Apr. 2014. Accessed Apr. 2014 <www.businessweek.com>

[21] Ibid.

[22] Ibid.

[23] *Roadmap to Achieve Energy Delivery Systems Cybersecurity.*

[24] Ibid.

[25] Lawrence, Dune.