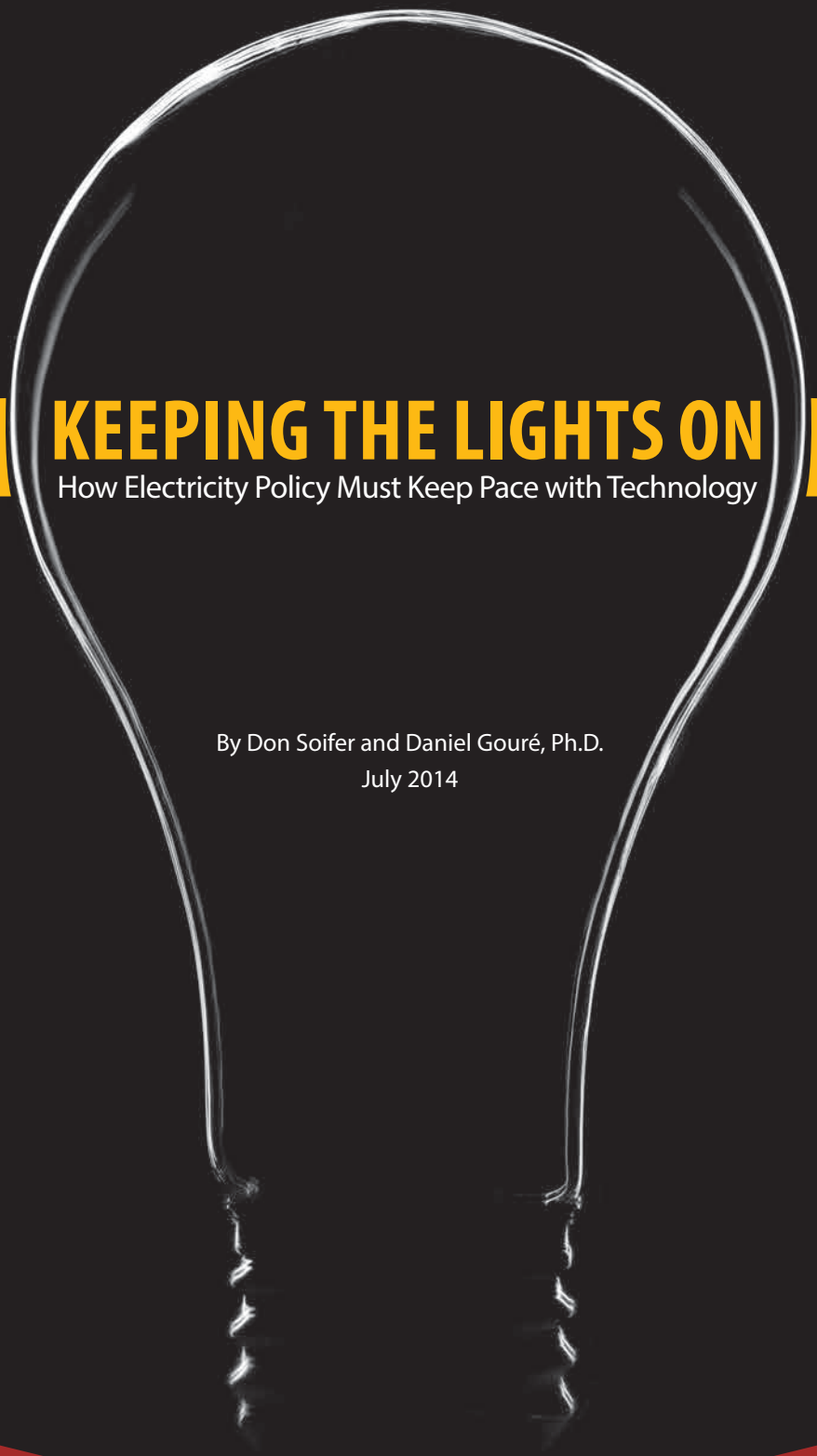


KEEPING THE LIGHTS ON

How Electricity Policy Must Keep Pace with Technology

By Don Soifer and Daniel Gouré, Ph.D.

July 2014

FUTURE OF THE POWER GRID SERIES

Lexington Institute

EXECUTIVE SUMMARY

The basic functions of American society and economy are reliant upon uninterrupted access to electricity to an unprecedented degree. Meanwhile, requirements for systems that safeguard power reliability and quality have become more complex amid sweeping changes in the electricity sector itself.

This paper focuses on three pressing areas where advancing solutions to bolster grid resilience will depend on electricity policies that keep pace with technology and markets:

Energy Storage. The present U.S. power grid lacks any large-scale electricity storage capacity, but new advances in technology suggest that its addition could represent a valuable strategy to manage peak demand, smooth volatility from renewable energy sources, and avoid damaging disruptions.

Microgrids. New microgrid initiatives in a number of states promise the ability to maintain power to critical entities during power-loss incidents, as well as integrating multiple energy sources, including renewables.

Cybersecurity. Potentially the most dangerous, but least understood, threats to the nation's power grid come from largely unknown actors with increasingly sophisticated methods.

The paper concludes with a discussion of ten specific, imminent challenges for decisionmakers seeking to implement public policies to support critical advances in each of these areas.

Details follow.

The Authors

Don Soifer is Executive Vice President of the Lexington Institute.

Dr. Daniel Gouré is Vice President of the Lexington Institute.

INTRODUCTION: NEW CHALLENGES, CHANGING MARKETS

America's economy and society are too dependent upon uninterrupted electric power to rely on the decentralized process that produced the present U.S. power grid to adequately ensure its protection. This task requires updated strategies for the technology, resources and mechanisms to integrate them, and also public policies that support sustained investment.

As our daily functions increasingly integrate technology (or are immersed in them entirely), Americans have become reliant on our continuous electricity supply. At the same time, proliferating varieties of complex and potent threats require intricate solutions that depend on planning, cooperation, and investment. Effective solutions must adapt not only to the risks themselves, but to the evolving power industry and its capacity to confront them.

Decisionmakers responsible for the public policies to support such solutions must also guard against stifling innovation. As early adaptors tend to drive new policies, attention must be paid to ensuring that this dynamic does not benefit their work at the expense of future innovations. Investors, legislators and regulators alike will make decisions informed by how the policy framework answers key questions, including:

- Who will be responsible for implementing, maintaining, and paying for the required improvements?
- Which authorities will be assigned responsibility for their supervision and regulation, and how will their jurisdictions be defined?
- How will the new initiatives be financed, and will parameters be established for new business models addressing cost recovery, profit and other factors that will attract sustained investment?

For decades, safeguarding electricity has largely focused on reinforcing physical assets: cutting back tree limbs, buttressing substations against flooding, etc. These strategies are no less critical today, as residential and small business customers are reminded with every strong thunderstorm.

But the diversity of potential threats to the grid requires multilayered strategies to defend it. For instance, cybersecurity, burying transmission lines underground, stocking critical spare parts, and contingency strategies for reconfiguring electricity transmission are increasingly elements of plans reviewed by state regulatory bodies, which must also determine who must pay for them.

This analysis focuses on three prominent solutions being pursued to bolster grid resilience in the United States: large-scale energy storage, the establishment of microgrids and cybersecurity.

Each involves a range of different actors working in multiple contexts, often responding to disassociated and dissimilar requirements. But in this new environment, where protection of the grid relies on combined, if not always coordinated efforts, there is a need for an updated policy framework to support this critical work.

THE NEW LANDSCAPE OF GRID RESILIENCY STRATEGIES

Vast changes in the United States' electric power industry frame the conditions and define the requirements today's grid must address. Over 3,200 different electricity providers serve U.S. customers today.[1] Most are power utilities, which are traditionally vertically-integrated monopolies that are averse to taking risks. For power utilities in the new electricity marketplace, risks can come from both the threat of attack or innovation itself.

Throughout history, geography frequently plays a role in technical innovation, and the power grid is no exception. California, home to many of the industry's early adaptors of new solutions, continues to

Hoboken, NJ endured massive flooding and crippling power outages in the aftermath of Hurricane Sandy in 2012

inform energy policies across the U.S., placing greater weight on the potential of its decisions, either deliberately or inadvertently, to impact other directions nationally. This scenario aptly describes the growth of large-scale energy storage projects.

Storage

Last year, the California Public Utilities Commission approved the nation's first statewide plan to create energy storage capacity. The regulator imposed a mandate with incentives for all investor-owned power utilities to create 1,325 megawatts of energy storage by 2020 – enough to provide power for a million homes for just over an hour.

New York and New Jersey, the two states hit hardest by Hurricane Sandy in 2012, are currently pursuing new strategies that decisionmakers hope will provide powerful protection against major incidents in the future.

New York seems likely to be the second state to implement such a plan. Governor Andrew Cuomo has made a policy priority of building energy infrastructure with an eye on strengthening its protections against interruptions from severe weather and other threats.

The New York City metropolitan area, the nation's most populous for the past 200 years, is in need of new solutions to replace its largest nuclear reactor, Indian Point, expected to close in the next few years. Utility Con Edison is proposing to ease the strains of peak energy use periods with a comprehensive initiative that will employ energy storage, energy efficiency and demand response plans that utilize flexible pricing to incentivize changes in energy use patterns.

New utility-scale energy storage initiatives add an entirely new dimension to the U.S. power grid – one that offers the short-term ability to help meet peak demand with continuity of service. Advocates of electricity from renewable sources like solar or wind recognize the benefits of being able to store energy generated when the sun is shining or the wind blowing for later use.

Today's large energy storage projects rely on technologies including lithium-ion and lead-acid batteries and other fuel cells, wind turbines, thermal storage and compressed air.

The U.S. Department of Energy has invested in one New York City intelligent energy storage system at a 7-Eleven convenience store in Flushing, Queens. The 100-kilowatt GreenStation developed by Green Charge Networks uses lithium-ion battery technology along with a system controller that allows it to reduce peak electricity demand by as much as 50 percent during summer months.[2]

While a single convenience store cannot hold the solution for the entire metropolitan area, the model illustrates how policymakers have chosen to take on some of these critical challenges. Ramping up adoption of solutions that can make a difference on a citywide scale will require a much more robust industry commitment to invest.

New Models for Changing Markets

The Queens GreenStation project utilizes battery storage as a tool to manage demand. Nationally, the power industry has largely relied on large power generation plants, operating on coal or other fossil fuels, to provide grid-critical services like voltage control. As these plants are displaced by small, distributed power generators, new models for providing these functions are necessary.

Another factor driving industry change is the growing majority of states implementing aggressive mandates requiring fast-approaching targets for increasing the share of their electricity produced from renewable sources. These plans, while popular among environmentalists, sharply impact the ability of utilities to recover investment costs under the old model.

The nation's grid relies on functions provided at critical points that have historically come from entities that no longer expect to play these same roles. Future reliability will depend on how regulators can utilize standards and other tools to fit the changing business landscape.

"If you have a 500-megawatt coal plant that supports transmission surrounding it, you can't take 500 megawatts of solar power in the same place and expect everything to work," observed John Moura, an official at the North American Electric Reliability Corporation.[3]

"If you have a 500-megawatt coal plant that supports transmission surrounding it, you can't take 500 megawatts of solar power in the same place and expect everything to work."

- John Moura, North American Electric Reliability Corporation

As costs ease downward, investor-owned utilities expect to recover the costs of their investments and also earn future profits from the projects. Southern Company CEO Tom Fanning recently characterized decision making priorities in an interview with EnergyWire, "So long as we stay true to the value-as-a-function-of-risk/return kind of dogma, long-term bilaterals, creditworthy counterparties, no fuel risk, no transmission risk, I'm all in."[4]

Resolving the details falls mostly to state utility regulators, who must balance fairness of charges to their monopoly consumers while safeguarding against cross-subsidization that can produce market distortions harmful to consumers. Systemic interdependencies across the power grid further increase the implications of regulators, whether at the state or federal level.

The ability of a utility to recover the costs of major assets used in the grid has historically been projected over 30 years, notes an analysis by the Edison Electric Institute. But in the new electricity markets, some rate-paying customers may be able to exit markets entirely, along with their burden for assisting cost recovery.[5] "The paradox is that customers leaving the grid will compound the issue of fixed cost recovery driving rates higher on a declining delivery revenue leading to potentially more customers leaving, and ultimately, a 'death spiral.'"[6]

This can happen on a large or small scale, so an appropriate pricing system to assign costs must fit the grid's new business realities. A compelling example of how new dynamics might look comes from a project between NRG Energy and Dean Kamen, the creator of Segway personal, motorized vehicles, on a natural gas power generator that would enable consumers to "completely sever ties with their electric utility."[7]

Power producers and their investors find it increasingly difficult to predict who their competition will be, and whether they will be competing fairly. This illustrates the added pressure on regulatory regimes to demonstrate responsiveness to changing electricity market dynamics.

Microgrids

The concept of microgrids is not new: any homeowner with a gas-powered generator has effectively established their own microgrid. Advances in technology have begun to make it possible for microgrids to play prominent roles in grid resilience strategies, presenting new policy challenges to support this role.

The Department of Defense has long recognized the unacceptable vulnerabilities of military bases that are entirely dependent on the commercial power grid, and has pursued strategies to reduce risks through greater energy independence. Some of these initiatives produce energy which can be sold to the commercial grid when not being used by the base, and include:

- Storage technology like S&C Electric's PureWave Storage Management System or L-3 Westwood's Load Demand Start Stop that function as their own microgrids for Army expeditionary camps.
- Distributed energy genetration from diverse sources, including solar, wind, natural gas, geothermal, and combined heat and power systems.[8]

On Miramar Marine Corps Air Station in San Diego, Raytheon's Integrated Defense Systems and partner Primus Power have developed a microgrid equipped with zinc-bromide battery storage capabilities integrating a 230-kilowatt photovoltaic solar system.[9]

Coordinated policy development between state and federal regulators and local authorities is critical to the success of microgrid strategies.

Quality of power is another valuable consideration for microgrids. "Lower-quality power is okay for some applications," notes Cheryl Martin, Acting Director of the Department of Energy's Advanced Research Projects Agency-Energy. "But suppose you wanted to back up your hospitals; there are many different ways you could use microgrids for a combination of reliability and robustness as well as pure islanding."[10]

In Hoboken, New Jersey, directly across the Hudson River from New York City, plans are taking shape to institute a microgrid that would provide parts of the city with its own power supply in the event of a major interruption or during especially peak periods of electricity use.

The Hoboken project is a joint undertaking by Sandia National Laboratories, utility PSE&G, the state public utilities board, and other partners. Plans for the microgrid would allow it to utilize a diverse array of different energy sources: fossil fuels with combustion engines, solar panels, wind turbines, and hydrogen fuel cells.

Because microgrids have the capacity to incorporate diverse energy sources, they hold appeal for meeting carbon emissions goals. This distributed generation allows microgrid operators the flexibility to purchase energy from a wide range of different technologies that utilize natural resources as well as capital accessed through different business models.

Microgrids can integrate power produced from different sources, including solar.

Under the Hoboken plan, compliance with national interconnection standards allow the Hoboken power sources to either be connected to the main PSE&G grid when the local grid is not in use, or to the microgrid when needed.

Cost estimates for the plan range from $30 million to over $50 million.

Coordinated policy development between state and federal regulators and local authorities is critical to the success of microgrid strategies. Enacting the plan will require the New Jersey Board of Public Utilities to rule on a number of complex issues, including who will pay for and control the required assets.

In May 2014, the state board concluded a 15-month-long case over utility PSE&G's Energy Strong proposal, approving $1.22 billion in resiliency spending covering both electricity and natural gas. The state's Division of Rate Counsel had pressed hard against what it argued were excessive consumer rate increases, contributing to an outcome far below the $2.6 billion the utility had sought. The plan will be paid for through rate increases to PSE&G's 2.2 million customers, expected at between one and two percent over current rates.[11]

Connecticut, as its neighboring states struggled to restore power in the aftermath of Hurricane Sandy, began its own statewide microgrid strategy, the nation's first. The state legislature approved microgrids in a 2012 law and subsequently passed clarifying statutes. The state provided funding to establish nine microgrid projects.

Cybersecurity

The ability to generate and move electric power is the centerpiece of any modern civilization. Without power there would be virtually no communications, water supplies, food harvesting, processing or storage, or industrial production. This is why the security of the power grid against both physical and non-physical attacks is so important.

Today's power grid is vulnerable to a variety of threats, the least understood but potentially most dangerous of which is cyber attack. The U.S. electricity grid is under near constant attack from malware, cyber-criminals and even foreign states. Intelligence agencies are concerned that some

foreign countries, including China, have been conducting cyber reconnaissance of the power grid in order to identify weakness and possibly even leave behind malware that can be activated in the event of conflict with the United States.

By some estimates, the national power grid is subjected to 10,000 attempted cyber attacks or intrusions every month. A recently-declassified 2008 Presidential Directive noted that "hackers and insiders have penetrated or shut down utilities in countries on at least three continents." It cited costs of these attacks to U.S. citizens and businesses of tens of billions of dollars each year.[12]

So-called Dragonfly malware espionage attacks compromised the computer systems of more than 1,000 energy companies in the United States and Europe.

Recent accounts of cyber attacks believed to originate from a collective of Eastern European hacker organizations known as Dragonfly found that malware espionage attacks compromised the computer systems of more than 1,000 energy companies in the United States and Europe. Symantec security experts observed that the attack "bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability."[13]

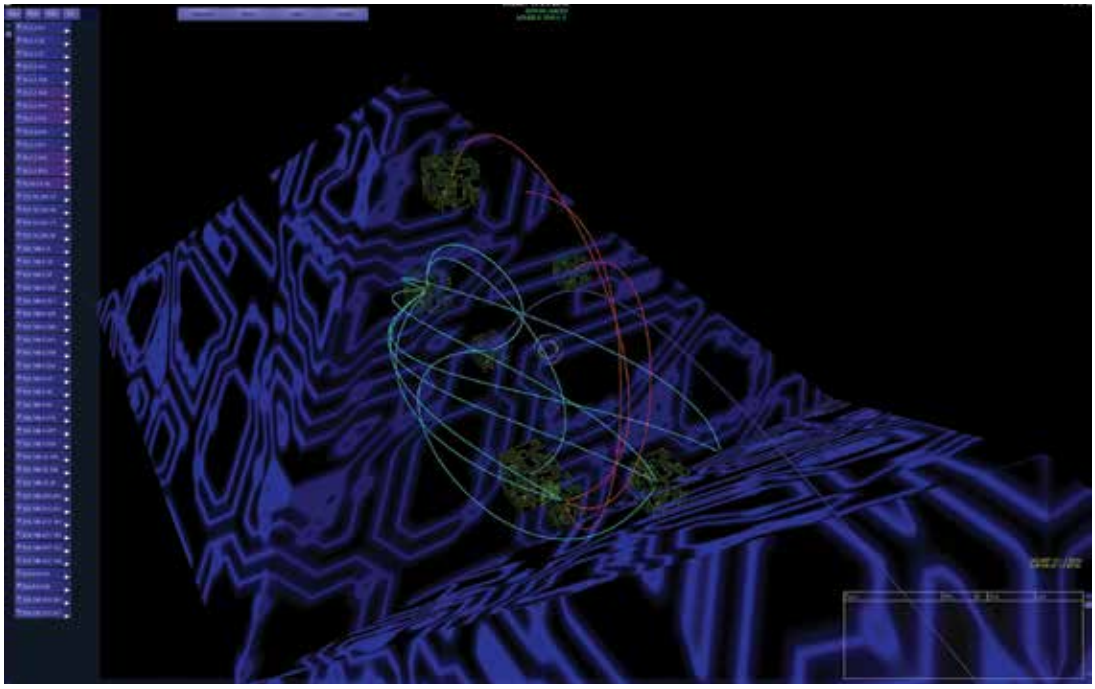
In testimony before the Senate Energy and Natural Resources Committee, Gerry Cauley, president of the North American Electric Reliability Corporation (NERC), stated that "I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures."[14]

The threat is likely to grow substantially worse even as our dependence on power increases. The proliferation of power generation sources, energy storage media and sensor systems in homes and businesses could make tomorrow's power grid even more vulnerable to cyber attack. Our experience with cyber intrusions and hacking has taught us one fundamental lesson: every IT system and network is only as strong as its weakest link. In a world in which microgrids, smart meters in individual homes and businesses and even cars are linked into the national power grid, the risk of cyber attack to that system will grow exponentially.

At present, most utility companies implement only the barest minimum of security measures. There is no centralized database of attacks on which utilities or local and state governments can rely for estimates of the character and severity of the cyber threat. There is no nationally-accepted set of standards for cybersecurity of the power grid. Looking ahead, who will set standards for the cybersecurity of smart meters, microgrids and electric cars?

"The dynamic relationship between standards and Smart Grid infrastructure dictates that standard setting itself should be an evolving process," notes Joel Eisen, University of Richmond Professor of Law in the Harvard Environmental Law Review. "Like standards themselves, the structure has to be flexible and accommodate change."[15]

The Department of Homeland Security (DHS) has responsibility for cybersecurity of U.S. critical infrastructure, including the electric power grid. However, DHS relies largely on industry to protect itself. As a result, the utilities and transmission companies tend to take only such measures as are required under the minimal standards established by NERC. According to a report released last year by Congressmen Ed Markey and Henry Waxman, only 21 percent of investor-owned utilities, 44 percent of municipal or cooperatively-owned utilities, and 62.5 percent of federally-owned utilities said they had taken any additional, voluntary measures.



The SOPHIA cyber security software developed at Idaho National Laboratory provides multiple ways for operators to view conversation pathways on their networks.

What else should be done? The Department of Energy has published an Energy Delivery Systems Cybersecurity Roadmap which calls for, *inter alia*, facilitating public-private partnerships to accelerate cybersecurity efforts for the grid of the 21st century; funding research and development of advanced technology to create a secure and resilient electricity infrastructure; supporting the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities and; facilitating timely sharing of actionable and relevant threat information. However, the federal government has not put much actual effort or resources behind any of these recommendations.

"Like standards themselves, the structure has to be flexible and accommodate change."

- Joel Eisen, University of Richmond.

It is vital that the development of an open architecture not only provide protection against threats to the grid, but integration that will not exclude new participants, energy sources and storage options.

Thus, it is up to the private sector as well as state and local governments to take the initiative and make their portions of the power grid more secure. According to a report by the Bipartisan Policy Institute, energy companies should create a new industry-led body to deflect cyber threats to the electric grid – from large generators to local distribution utilities. State and local regulators should work with this body to develop common cybersecurity standards, create metrics by which to evaluate utility investments in cybersecurity and even establish cost-recovery modalities for such investments.[16]

The National Security Agency in Fort Meade, MD, home to many cybersecurity initiatives.

10 CHALLENGES FOR NEW ELECTRICITY POLICIES

Establishing a consistent regulatory climate that supports long-term investment strategies will be crucial to solutions taking hold successfully. Access to competitively-priced capital will largely shape the energy options available across markets, along with natural gas, wind and sun. Hurdles to sustained investment strategies can include variations in national markets (natural gas) and regional ones (weather, uneven increases in electricity prices), as well as managing the intended and unintended impacts of government programs incentivizing certain technologies over others.

Other challenges facing decisionmakers include:

1. Regulatory jurisdiction over grid assets, including transmission lines, is uncertain when they cross state lines, potentially triggering the Federal Energy Regulatory Commission's authority to rule on how projects are financed and rendering implications for state utility boards uncertain.
2. Establishing consistent, accepted business models, including pricing, for grid storage systems will be essential to both attracting investment and allowing regulators to implement best practices.
3. Regulation of microgrids is a murky domain. Microgrid governance issues depend on whether they are established as legal entities, how ownership of assets is defined, and how they fit into established regulatory regimes.
4. Contractual arrangements between utilities and microgrids must be developed to provide level playing fields for developers, providers and utilities. Adequate transparency must permit regulators to ensure that monopoly customers are not overcharged.
5. Local governments, which do not control their power grids or own their assets, must coordinate decision making with other authorities. This poses major obstacles for the financing of microgrids, while raising other challenges, like resolving questions of land use and access. How will maintenance or upgrades for shared entities be assigned?

6. The impact of microgrids on the 43 states that currently have net metering rules in place must be resolved. To the extent that microgrids are in fact compatible with states' net metering laws, providers will share their energy between commercial and microgrids. How will this impact their compensation under state laws?
7. Outdated core infrastructure carries most of the electric power across the U.S. today. Such technology is often patched but rarely redesigned or modernized, resulting in lost productivity and power outages. Stockpiling critical spare parts, and integrating more interchangeable parts across the system, will diminish both the likelihood of interruptions and the magnitude of events when they do occur.
8. Unions representing grid workers frequently weigh in on power grid regulatory cases, and place the workplace issues of members above other considerations like grid resilience.
9. The development of technology is not a linear process. As government incentives continue to reward investment in certain technologies and fuel sources, it will be essential that private capital be able to flow to those who can navigate market-creating factors, while removing obstacles. It is to be expected that early innovators will drive broadly-adopted solutions. Government decisionmakers must be mindful of the risks of their actions stifling innovations of other kinds.
10. Development of consistent standards is critical for the power grid's cyber security. This is particularly important as the current power grid and its management systems become more open, reflecting the array of technologies and software programs available to producers, grid managers and users alike. The more open the architecture, the greater the need for common standards.

END NOTES

1. American Public Power Association, *2014-15 Annual Directory and Statistical Report*.
2. U.S. Department of Energy Global Energy Storage Database, http://www.energystorageexchange.org/projects/521 (accessed May 24, 2014). Also: "Power Efficiency Case Study," Green Charge Networks, www.greenchargenet.com.
3. Peter Behr, "Operators Seek Technology Fixes for Power Mix's Metamorphis," EnergyWire (May 15, 2014).
4. Rod Kuckro, "Southern Company CEO Mulls Entry Into New Markets," EnergyWire (May 19, 2014).
5. Peter Kind, "Disruptive Challenges: Financial Implications and Strategic Responses to a Changing Retail Electric Business," Edison Electric Institute (January 2013).
6. California Institute of Technology Resnick Institute, "Grid 2020: Towards a Policy of Renewable and Distributed Energy Resources," (2012), p. 29.
7. Reuben Brewer, "Is This the Electric Utility 'Apocalypse?'" The Motley Fool (May 18, 2014).
8. David Chiesa, "Striving for Certainty," DoD Power and Energy (Spring 2014).
9. U.S. Department of Energy Global Energy Storage Database, *op cit*.
10. "Unrestricted Innovation: Ideas Spotlight ARPA-E," Interview with Dr. Cheryl Martin, *DoD Power and Energy* (Spring 2014), p. 12.
11. Tom Johnson, "After Yearlong Debate, BPR Approves PSE&G 'Energy Strong' Initiative," NJ Spotlight (May 22, 2014).
12. National Security Presidential Directive #54/Homeland Security Presidential Directive #23 (January 9, 2008), p. 2.
13. "Energy Firms Hacked by Cyber-Espionage Group Dragonfly," BBC News (July 1, 2014).
14. Gerry Cauley, Testimony before the U.S. Senate Energy and Natural Resources Committee (April 10, 2014).
15. Joel B. Eisen, "Smart Regulation and Federalism for the Smart Grid," *Harvard Environmental Law Review* (Vol. 37. 2013), p. 50.
16. "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," Bipartisan Policy Center (February 2014).

1600 Wilson Boulevard, #900
Arlington, VA 22209

Telephone: 703-522-5828
Fax: 703-522-5837
Web: www.lexingtoninstitute.org
mail@lexingtoninstitute.org