PROTECT OUR POWER

Quadrennial Energy Review (QER)

Executive Summary

- The DOE released its second installment of the **Quadrennial Energy Review (QER)** on Friday, January 6, 2017. This installment focuses entirely on the electrical grid, and outlines three core, integrated objectives: maximizing economic value, integrating renewable energy generation, and importantly for us, enhancing grid security and resiliency.

Links to the full report and executive summary are below, but here are the main conclusions from the report concerning security and resiliency:

- The reliability of the electric system underpins virtually every sector of the modern U.S. economy. The changing nature of the grid (new technology) as well as the changing nature of threats facing it creates a need to update and evolve current reliability metrics.

- Electricity outages disproportionately stem from disruptions on the distribution system (over 90 percent of electric power interruptions), both in terms of the duration and frequency of outages; this is largely due to weather-related events. Damage to the transmission system, while infrequent, can result in more widespread major power outages that affect large numbers of customers with significant economic consequences.

- The leading cause of power outages in the United States is extreme weather, including heat waves, blizzards, thunderstorms, and hurricanes. Events with severe consequences are becoming more frequent and intense, due to climate change, and have been the principal contributors to an observed increase in the frequency and duration of power outages in the United States.

- The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures. Mitigation and response to cyber threats are hampered by inadequate information-sharing processes between government and industry, the lack of security-specific technological and workforce resources, and challenges associated with multi-jurisdictional threats and consequences. System planning must evolve to meet the need for rapid response to system disturbances.

- There are no commonly used metrics for measuring grid resilience. Several resilience metrics and measures have been proposed; however, there has been no coordinated industry or government initiative to develop a consensus on or implement standardized resilience metrics.

This installment provides 76 recommendations across the three objectives. Below are those related to security and resiliency:

- **Protect the Electricity System as a National Security Asset.** The Federal Power Act, as amended by the FAST Act, should be further amended by Congress to clarify and affirm the Department of Energy's (DOE's) authority to develop preparation and response capabilities that will ensure it is able to issue a grid-security emergency order to protect critical electric infrastructure from cyber attacks, physical incidents, EMPs, or geomagnetic storms. In the area of cybersecurity, Congress should provide FERC with authority to modify NERC-proposed reliability standards—or to promulgate new standards directly—if it finds that expeditious action is needed to protect national security in the face of fast-developing new threats to the grid.

    - Collect information on security events to inform the President about emergency actions as well as imminent dangers. DOE should collect targeted data on critical cyber, physical, EMP, and geomagnetic disturbance events and threats to the electric grid to inform decision making in the event of an emergency or to inform the anticipatory authorities in the FAST Act.
    - Adopt integrated electricity security planning and standards. FERC should, by rule, adopt standards requiring integrated electricity security planning on a regional basis to the extent consistent with its statutory authority.
    - Assess natural gas/electricity system infrastructure interdependencies for cybersecurity protections. DOE, pursuant to FAST Act authorities and in coordination with FERC, should assess current cybersecurity protections for U.S. natural gas pipelines and associated infrastructure to determine whether additional or mandatory measures are needed to protect the electricity system.

- **Increase Financing Options for Grid Modernization.** Estimates of total investment requirements necessary for grid modernization range from a low of about $350 billion to a high of about $500 billion.
    - Expand DOE's loan guarantee program and make it more flexible to assist in the initial deployment of innovative grid technologies and systems.

- **Support Industry, State, Local, and Federal Efforts to Enhance Grid Security and Resilience.**
    - Develop uniform methods for cost-benefit analysis of security and resilience investments for the electricity system.
    - Provide incentives for energy storage.
    - Support grants for small utilities facing cyber, physical, and climate threats.
    - Support mutual assistance for recovering from disruptions caused by cyber threats.
    - Support the timely development of standards for grid-connected devices.
    - Require states to consider the value of DER, funding for public purpose programs, energy and efficiency resource standards, and emerging risks in integrated resource or reliability planning under PURPA.

- **Improve Data for Grid Security and Resilience.** Enhance coordination between Energy Sector Information Sharing and Analysis Centers (ES-ISACs) and the intelligence communities to synthesize threat analysis and disseminate it to industry in a timely and useful manner.

- Here are links to various parts of the QER for reference:
    - QER Home
    - QER Full Report
    - QER Summary for Policy Makers
    - QER Section IV: Ensuring Electricity System Reliability, Security, and Resilience
    - QER Conclusions and Recommendations