wiley

NEWSLETTER

Electricity Supply Cybersecurity Concerns Create Business Opportunities

November 2013

At the end of October, the Eastern Interconnection Planning Collaborative (EIPC) began planning for the expected shutdown of more coal plants and increased production of energy with wind power and shale gas-powered generation. EIPC focuses on assuring adequate and secure transmission of electricity and includes electric system planners' representatives and representatives of utilities and the Tennessee Valley Authority. Past EIPC planning projects, funded by an American Recovery and Reinvestment Act grant, brought together grid officials from the Eastern Interconnection, the synchronized high-voltage power network that runs from east of the Rocky Mountains to the Atlantic Coast.

Next, this group may look at measures to ensure that sufficient future pipeline capacity exists for gas-fired power plants (including northeastern states) if the broad switch from coal to gas plants continues. It also may decide to study (with private, not U.S. Department of Energy (DOE) funds) how efficiently and safely large amounts of power could move through the region under various scenarios. But ensuring security of that transmission is likely to move higher on the agenda.

These efforts merit attention not only from companies involved in energy generation and transportation, but from suppliers who can help support redundancies and other techniques likely to be put in place to improve security.

EIPC's activities will reflect pressure from the Administration. Most directly, the new Energy Secretary, Ernest Moniz, has been focusing on cybersecurity and related protections whenever he addresses infrastructure development. Under Moniz, therefore, DOE can be expected to work with the Federal Energy Regulatory Commission to build out a "21st century" power grid and intensify its efforts to identify vulnerabilities in the nation's integrated power systems.

Among the most important facets of that vulnerability, according to Moniz, are cyberthreats and extreme weather. Thus, substantial efforts to address the February 2013 Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience" can be expected from DOE.

This presidential guidance and the resulting efforts build on President Obama's warning in his State of the Union Address:

America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

They also reflect the fact that in August, the White House announced that it was looking into ways to incentivize the energy and water sectors to adopt new standards designed to thwart cyberattacks, including insurance and priority consideration for grants and technical assistance. President Obama has already ordered the Departments of Homeland Security (DHS), Commerce, and the Treasury to identify ways to encourage the energy industry to comply with EO 13636 calling on utilities, telecommunications firms, and transportation companies to voluntarily adopt security standards. Now DOE and EIPC can be expected to join in this effort.

According to the White House, its policies are intended to strengthen the security and resilience of critical infrastructure against evolving threats and hazards, while incorporating strong privacy and civil liberties protections into every cybersecurity initiative. President Obama has called for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical assets.

Sources at DOE and FERC indicate that the incentives to be considered include preferences for compliant companies in awarding federal critical infrastructure grants, protecting information sharing, streamlining regulations, and publicly recognizing companies that participate. In addition, research and development support and creating a "competitive cyber-insurance market" have been considered for companies that agree to comply with a risk-reduction program managed by DHS.

While some of the work necessary to address these concerns will focus on computer coding and intrusion warning, ensuring adequate system reliability through use of reliable but innovative technologies and adequate redundancy also will be key elements. These facts should provide significant business opportunities to energy storage and electronic controls providers, among others.