CLIENT ALERT

NIST Publishes Cybersecurity Framework Smart Grid Profile

Jul.29.2019

The U.S. electric power grid is modernizing through "smart" technologies, such as advanced metering infrastructure and automated distribution management systems. These changes bring benefits to the grid and customers, but also present potential cybersecurity risks. Energy industry stakeholders and smart / connected technology developers should closely monitor changes and guidance in this area, such as the National Institute of Standards and Technology's (NIST) recently published Smart Grid Profile. (NIST is a non-regulatory agency of the U.S. Department of Commerce, whose mission includes promoting innovation and industrial competitiveness through science and technology, engineering, and information technology.)

The Smart Grid Profile is NIST's "initial attempt to apply risk management strategies from the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to the smart grid." The Profile provides numerous and detailed cybersecurity considerations for power system owners/operators in each of the Cybersecurity Framework's five Core areas: "identify, protect, detect, respond, and recover." Like most iterations of the Cybersecurity Framework, applying the Profile is voluntary. But with enough industry adoption, it may become a default best practice.

In applying the five Core areas to "smart grid" technologies, the Profile recognizes that the major business interests of power system stakeholders are maintaining safety, maintaining power system reliability, maintaining power system resilience, and supporting grid modernization. The Profile was developed to provide power system owners/operators with concrete steps and strategies to safeguard those business interests through each of the five Core areas:

- **Identify** risks by being highly familiar with hardware and software assets; understanding the organization's placement in grid infrastructure; assessing power system dependencies and supply chain dependencies; conducting thorough risk assessments; understanding applicable regulations and policies; evaluating potential threats; and developing risk management strategies and policies.
- **Protect** the system by limiting access to sensitive systems and information to the appropriate personnel; authenticating devices before connecting to the grid network; implementing robust training programs for personnel; utilizing proper data security measures; maintaining and updating equipment; and providing appropriate protective technologies.
- **Detect** potential threats by establishing alert thresholds to identify anomalies and events; monitoring systems and personnel for unexpected behaviors; implementing policies and processes to detect threats and events; and continuously improving detection and monitoring systems.
- **Respond** to events by developing and executing effective response processes; having established communication routes for reporting events; prioritizing information sharing during an event; investigating and analyzing information surrounding the event; mitigating further impacts; and developing and implementing lessons learned from previous events.
- **Recover** from an event by implementing an established recovery plan; improving systems to combat exposed vulnerabilities; and maintaining open communication.

The Profile is an important contribution to an evolving national discussion aimed at enabling power system owners/operators to prioritize organizational cybersecurity activities to align with their available resources, engage in better informed decision making about cybersecurity activities, convey cybersecurity requirements to third parties such as supply chain vendors, and benchmark the strength of their cybersecurity systems against the five Core values.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com