MOODY'S
INVESTORS SERVICE

SECTOR COMMENT
14 October 2019

Rate this Research

Contacts

Nana Hamilton +1.212.553.9440
AVP-Analyst
nana.hamilton@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Michael G. Haggarty +1.212.553.7172
Associate Managing Director
michael.haggarty@moodys.com

Jim Hempstead +1.212.553.4318
MD-Utilities
james.hempstead@moodys.com

Utilities and power companies – US

GAO's call for improved electric grid cybersecurity oversight is credit positive, but highlights vulnerability risk

On 25 September, the US House Committee on Energy & Commerce released a Government Accountability Office (GAO) report recommending that the federal government strengthen cybersecurity standards and compliance thresholds for the US electric grid. The GAO's call for improved cybersecurity oversight is credit positive for US electric utilities because it would help improve the grid's ability to withstand cyberattacks. But the GAO's recommendations, even if fully implemented, do not eliminate cyber risk for the power grid.

We continue to see cybersecurity as a growing risk for the utilities sector. The GAO's report highlights this risk, and although implementation of the recommendations would be credit positive, regulatory compliance alone does not sufficiently defend against cyber risk. We assess the overall cyber risk of the electric utilities sector as medium-high (see "Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects").

The GAO report finds that Department of Energy (DOE) strategies for addressing electric grid cybersecurity and mandatory grid standards and associated thresholds approved by the Federal Energy Regulatory Commission (FERC) do not adequately address the cybersecurity risks facing the electric grid. The electric grid's vulnerability to sophisticated cyber attacks is a material credit negative for the sector.

The GAO recommends that the DOE and FERC take actions to bolster the grid's ability to withstand mounting cybersecurity risks (see "GAO Report to Congressional Requesters: Critical Infrastructure Protection - Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid"). Both the DOE and the FERC have agreed with the GAO's recommendations.

The responsibility for managing a utility's cyber risk resides with C-suite executives and the board of directors. But the prospect of additional regulatory oversight is positive because it will drive a heightened sense of urgency among utility executives and boards. That said, the reliance of many utilities on regulatory oversight to address their cyber risk exposure could create a culture of compliance that falls short of taking measures to reduce that risk.

With no precedent of malicious cyber-related large-scale power outages in the US, the extent to which a cyberattack could disrupt grid operations remains unclear. The DOE and FERC have performed various assessments of the potential scale of power outages that could result from a cyberattack. However, the GAO said that their conclusions about the scale of such outages may not be realistic, in part due to some of the underlying assumptions that were used. For example, officials contracted to conduct the DOE's Electricity Subsector Risk Characterization Study in 2017, 2018 and 2019 warned that their analyses used a model of the Western Interconnection that accounted for less than a quarter of the interconnection's actual capacity in 2018. As a result, the model could not accurately predict the behavior of the current system.

The GAO's recommendations to improve grid cybersecurity come at a time of heightened awareness of the broader US electrical system's vulnerability to cyberattacks. These vulnerabilities include the grid's reliance on other infrastructure, such as natural gas pipelines, which is also exposed to the risk of cyberattack. The US natural gas pipeline industry, despite having become the primary supplier of fuel to the US generation fleet, is not covered by federally mandated cybersecurity standards. FERC officials have expressed concerns about the need for improved cybersecurity oversight of interstate gas pipelines, which would be credit positive for pipeline companies and utilities (see "Electric and gas – US: Pipeline cybersecurity standards help plug security loophole in utility supply chain").

Cyberattacks on utility infrastructure are a form of event risk. For now, we view the potential financial impact of a cyber event as akin to the effect of destructive weather events. Both can disrupt service and cause widespread physical damage to critical utility infrastructure. A key difference is that cyberattacks typically strike without warning, while hurricanes and tropical storms are monitored by meteorologists who can estimate the time they will make landfall.

If a large-scale cyberattack were to strike a utility, extraordinary federal government intervention would be likely, much as it would be following a destructive storm, as was the case for Entergy New Orleans LLC (Ba1 stable) following Hurricane Katrina in 2005 and for New York, New Jersey and Connecticut utilities following Superstorm Sandy in 2012. Government intervention or support could include direct or indirect financial aid or the provision of other resources aimed at restoring a utility's operations (see "Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high").

Moody's related publications

Sector In-Depth

- Cyber Risk – Global Investment Banks: GIBs heighten readiness against constant cyber threat, October 2019
- Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, October 2019
- Local government – US: Ransomware attacks highlight importance of IT investment and response planning, October 2019
- Electric and gas – US: Pipeline cybersecurity standards help plug security loophole in utility supply chain, July 2019
- Cross-Sector - Global Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019
- Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high, September 2018

Topic Page

- Cyber Risk

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

REPORT NUMBER 1196846

Moody's
INVESTORS SERVICE