Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: Public Power Cyber Defenses Hardened Against Rising Threats

Fitch Ratings-Austin/New York-21 April 2022: Public power utilities are well-positioned to weather attacks due to the electric sector's years of attention to cyber threat mitigation and regulatory requirements, which offers a heightened level of protection relative to other infrastructure assets, Fitch Ratings says. Federal warnings of cyberattacks targeting US critical infrastructure coincide with news reports of Texas energy sector infrastructure system probes, which can be used to scan and monitor networks for weaknesses. Risks are amplified, and increased information technology investment and spending will be necessary.

The Department of Energy (DOE), CISA, National Security Agency, and the FBI jointly released an alert in mid-April to warn that certain advanced persistent threat (APT) actors are capable of gaining full system access to multiple industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices using custom-made tools that target ICS/SCADA. Electric utilities are exposed to these threats as they use ICS to connect into the electric grid and SCADA to gather and process data from substations. Events caused by operating technology (OT) breaches can threaten human safety and the availability of essential assets and are much more severe than IT breaches.

The costs to maintain and update cybersecurity will rapidly increase to keep pace with elevated ICS threats amid geopolitical tension. System lifecycles are decreasing along with rapid evolution of technology and sophistication of cyber intrusions. Strengthening of cyber hygiene culture through investment in human capital and technology is critical to continue effective mitigation of fast-evolving APT threats.

Electric utility critical assets have been hardened by over a decade of compliance with the North American Electric Reliability Corporation's (NERC) critical infrastructure protection (CIP) mandatory cyber hygiene security standards. Key elements of NERC CIPs include critical asset identification or cataloguing; security controls; background checks and training; electronic, physical and system security; incident management; recovery plans; change management and vulnerability assessments; and information protection. The level of federal attention and investment makes the electric sector uniquely experienced to manage cyber threats, much more than other critical infrastructure.

The Electric Reliability Council of Texas (ERCOT) manages the electric power grid for about 90% of Texas load. ERCOT collaborates with relevant government and industry agencies to protect the Texas electric grid from cyber threats. Two ERCOT working groups routinely meet to assess and address security risks. The Public Utility Commission of Texas (PUCT) and ERCOT contract with a third party to act as the PUCT's cybersecurity monitor to provide resources and report to the PUCT on cyber readiness.

The renewed emphasis on partnerships as threats increase is supported by platforms allowing utility operators to share cyber threats in real time without compromising competitive or sensitive information. Public power consortiums, such as the American Public Power Association and the

Large Public Power Council, provide their members with cybersecurity support programs. CISA and the FBI updated the CISA Shields Up program in March 2022, providing best practices, technical guidance, free tools and resources that are available to all organizations.

The ability to protect infrastructure from attacks is considered under Fitch's US public power rating criteria as part of Fitch's assessment of management quality and governance, which is an asymmetric credit factor where weaker characteristics may constrain a rating. Fitch assesses utilities' cyber security policies, investment and training; their maintenance of insurance against cyberattacks; and their protocols to address cyber incidents. No public power ratings are currently constrained by concerns regarding a utility management's lack of preparation. In the event of a cyberattack, Fitch would assess the effect on financial metrics and performance of halts in service, delays in revenue generation, ransomware payments or unexpected capital costs.

Contacts:

Omid Rahmani
Associate Director, US Public Finance
+1 512 215-3734
Fitch Ratings, 2600 Via Fortuna, Suite 330
Austin, TX 78746

Rebecca Meyer
Director, US Public Finance
+1 512 215-3733

Sarah Repucci
Senior Director, Fitch Wire
Credit Policy – Research
+1 212 908-0726

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email: sandro.scenga@thefitchgroup.com

The above article originally appeared as a post on the Fitch Wire credit market commentary page. The original article can be accessed at www.fitchratings.com. All opinions expressed are those of Fitch Ratings.Public Power Cyber Defenses Hardened Against Rising Threats
Thu 21 Apr, 2022 – 12:30 PM ET

Fitch Ratings-Austin/New York-21 April 2022: Public power utilities are well-positioned to weather attacks due to the electric sector's years of attention to cyber threat mitigation and regulatory requirements, which offers a heightened level of protection relative to other infrastructure assets, Fitch Ratings says. Federal warnings of cyberattacks targeting US critical infrastructure coincide with news reports of Texas energy sector infrastructure system probes, which can be used to scan and monitor networks for weaknesses. Risks are amplified, and increased information technology investment and spending will be necessary.

The Department of Energy (DOE), CISA, National Security Agency, and the FBI jointly released an alert in mid-April to warn that certain advanced persistent threat (APT) actors are capable of gaining full system access to multiple industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices using custom-made tools that target ICS/SCADA. Electric utilities are exposed to these threats as they use ICS to connect into the electric grid and SCADA to gather and process data from substations. Events caused by operating technology (OT) breaches can threaten

human safety and the availability of essential assets and are much more severe than IT breaches.

The costs to maintain and update cybersecurity will rapidly increase to keep pace with elevated ICS threats amid geopolitical tension. System lifecycles are decreasing along with rapid evolution of technology and sophistication of cyber intrusions. Strengthening of cyber hygiene culture through investment in human capital and technology is critical to continue effective mitigation of fast-evolving APT threats.

Electric utility critical assets have been hardened by over a decade of compliance with the North American Electric Reliability Corporation's (NERC) critical infrastructure protection (CIP) mandatory cyber hygiene security standards. Key elements of NERC CIPs include critical asset identification or cataloguing; security controls; background checks and training; electronic, physical and system security; incident management; recovery plans; change management and vulnerability assessments; and information protection. The level of federal attention and investment makes the electric sector uniquely experienced to manage cyber threats, much more than other critical infrastructure.

The Electric Reliability Council of Texas (ERCOT) manages the electric power grid for about 90% of Texas load. ERCOT collaborates with relevant government and industry agencies to protect the Texas electric grid from cyber threats. Two ERCOT working groups routinely meet to assess and address security risks. The Public Utility Commission of Texas (PUCT) and ERCOT contract with a third party to act as the PUCT's cybersecurity monitor to provide resources and report to the PUCT on cyber readiness.

The renewed emphasis on partnerships as threats increase is supported by platforms allowing utility operators to share cyber threats in real time without compromising competitive or sensitive information. Public power consortiums, such as the American Public Power Association and the Large Public Power Council, provide their members with cybersecurity support programs. CISA and the FBI updated the CISA Shields Up program in March 2022, providing best practices, technical guidance, free tools and resources that are available to all organizations.

The ability to protect infrastructure from attacks is considered under Fitch's US public power rating criteria as part of Fitch's assessment of management quality and governance, which is an asymmetric credit factor where weaker characteristics may constrain a rating. Fitch assesses utilities' cyber security policies, investment and training; their maintenance of insurance against cyberattacks; and their protocols to address cyber incidents. No public power ratings are currently constrained by concerns regarding a utility management's lack of preparation. In the event of a cyberattack, Fitch would assess the effect on financial metrics and performance of halts in service, delays in revenue generation, ransomware payments or unexpected capital costs.

Contacts:

Omid Rahmani
Associate Director, US Public Finance
+1 512 215-3734
Fitch Ratings, 2600 Via Fortuna, Suite 330
Austin, TX 78746

Rebecca Meyer
Director, US Public Finance
+1 512 215-3733

Sarah Repucci
Senior Director, Fitch Wire
Credit Policy – Research
+1 212 908-0726

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email: sandro.scenga@thefitchgroup.com