MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
10 July 2019

Rate this Research

TABLE OF CONTENTS

Contacts

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

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

Gavin Macfarlane +1.416.214.3864
VP-Sr Credit Officer
gavin.macfarlane@moodys.com

Sreedhar Kona +1.212.553.4199
VP-Senior Analyst
sreedhar.kona@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

Walter J. Winrow +1.212.553.7943
MD-Gbl Proj and Infra Fin
walter.winrow@moodys.com

Electric and gas – US

Pipeline cybersecurity standards help plug security loophole in utility supply chain

» **Calls for improved mandatory US cybersecurity standards for interstate natural gas pipelines are credit positive for pipeline companies and utilities.** The US natural gas pipeline industry, despite having become the primary supplier of fuel to the US power generation fleet, is not covered by federally mandated cybersecurity standards. This creates a significant vulnerability for US utilities, which have long been subject to mandatory cybersecurity standards. The implementation of mandatory standards for gas pipelines would force any late adopters to shore up their baseline defenses and become more difficult targets for attackers; as well as support pipeline operators ability to recover these costs through future rates and support their financial position.

» **Government oversight of natural gas pipeline cybersecurity practices are weak, but the ultimate responsibility for oversight resides with the board of directors.** A December 2018 Government Accountability Office (GAO) audit cited cybersecurity as a key weakness in the Transportation Security Administration's (TSA) natural gas pipeline security program. The TSA has the equivalent of only six full-time employees tasked with supervising the entire US interstate pipeline industry, which includes natural gas transmission pipelines, as well as pipelines transporting oil and other hazardous liquids. In addition, the number of TSA critical facility security reviews of pipeline facilities has fallen sharply since 2010.

» **Natural gas pipelines are prized targets for cybercriminals.** The increasing reliance of pipeline operators on sophisticated networked computer systems and electronic data leaves them vulnerable to attacks from cybercriminals, who have identified natural gas pipelines as a prized target. Operators are not currently required to report cyberattacks if they are not deemed material by the company. As a result, complete data on the number and scale of attacks is not readily available.

» **Interdependence between utilities and interstate natural gas pipelines is increasing.** The confluence of the shale revolution started in 2008 and environmental concerns that have led to the retirement of coal plants has contributed to the emergence of natural gas-fired power plants as the most significant power generation source in the US.

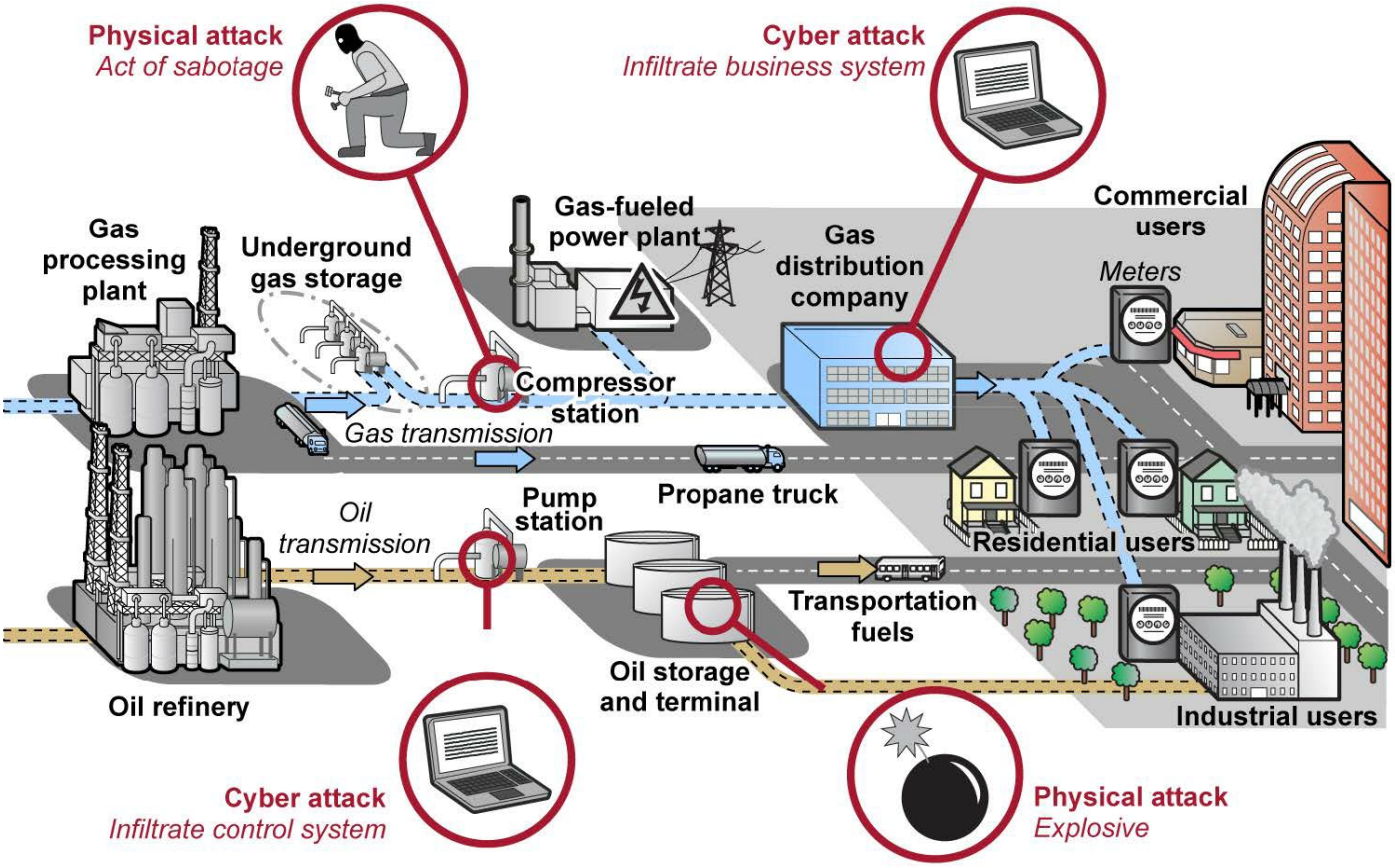
Calls for improved cybersecurity standards for natural gas pipelines highlights contrast with utility industry

Mounting calls for improved cybersecurity oversight of interstate natural gas pipelines are credit positive for pipeline companies and utilities. 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. By contrast, US utilities, because of the critical nature of their service, have long been subject to mandatory cybersecurity standards. The divergent standards applied to these two industries despite their tight linkage and dependency leaves a significant vulnerability in the utility industry's cyber risk management (Exhibit 1). Federal enforcement of stricter standards to protect pipelines from cyberattacks would help address this weakness.

Exhibit 1

Natural gas pipelines are the US electrical system's primary fuel supply transport vector

US natural gas and oil pipeline system's basic components and examples of vulnerabilities



Source: Government Accountability Office

At a June 12 hearing held by the US House Energy and Commerce Committee's energy subcommittee, Federal Energy Regulatory Commission (FERC) members Richard Glick and Cheryl LaFleur expressed concerns about the lack of mandatory cybersecurity standards for the US gas pipeline system, echoing more detailed remarks made in February by FERC Chairman Neil Chatterjee to the US Senate Committee on Energy and Natural Resources. Last October, the Department of Homeland Security (DHS) and the Department of Energy announced a "pipeline cybersecurity initiative" to assess the risks facing the gas pipeline sector.

The increased attention focused on the lack of stringent pipeline cybersecurity oversight highlights the marked contrast with oversight of the power sector. The US operating bulk electricity infrastructure became subject to mandatory North American Electric Reliability

Corporation Critical Infrastructure Protection (NERC CIP) standards in 2009. Since being adopted, these standards have undergone a series of revisions to address developing trends in cybersecurity and are now on their fifth version. NERC-CIP consist of nine standards and 45 requirements covering the security of electronic perimeters and the protection of critical assets as well as personnel and trainings, security management, and disaster recovery planning. Although these standards, by their nature, cannot be as dynamic as the cybersecurity threats themselves, they nonetheless provide a baseline cybersecurity strategy that utilities can build on to incorporate their own distinct requirements.

Federal oversight of cybersecurity standards in the utility industry was further tightened on June 20, when FERC voted to require utilities to report cyberattacks on the electric grid even when they do not disrupt service. Utilities were previously only required to report cyber intrusions if the attacks disrupted their ability to deliver electricity to customers. The new rule sets baseline requirements for what utilities must report.

We view mandatory cybersecurity standards as a starting point for protecting against cyber threats. The adoption of mandatory cybersecurity standards in the natural gas pipeline sector will help guarantee that all operators are focused on this growing risk (at least to the level required by law) and force any late adopters to shore up their baseline defenses and become more difficult targets for attackers, or face regulatory fines and increased oversight.

Furthermore, as a regulated asset, natural gas pipelines charge rates that can be adjusted through rate case proceedings to recover prudently incurred costs. Mandatory cybersecurity standards would support pipeline operator arguments of the need to increase investments in this area, which should strengthen their case for recovering these costs through future rates. This, in turn, would further support their financial position.

Government oversight of pipeline cybersecurity practices found to be lacking - but the responsibility for protection resides with the board of directors

A December 2018 Government Accountability Office (GAO) audit cited cybersecurity as a key weakness in the natural gas pipeline security program run by the Transportation Security Administration (TSA), which is in charge of cybersecurity oversight on all US interstate pipelines. More specifically, the GAO reported that the TSA's March 2018 strengthening of its voluntary pipeline security guidelines incorporated most, but not all, of the principles and practices from the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Moreover, the TSA does not have a documented process for reviewing and revising its guidelines on a regular basis, an issue the agency is now looking to remediate. The NIST Framework is broadly viewed as the gold standard for cybersecurity and the foundation for many new cybersecurity standards currently being developed.

DHS includes power generation in what it defines as the energy sector, which is one of 16 infrastructure industries that it has designated as being critical to US national security. DHS deems an infrastructure industry as being critical if incapacitation or destruction of its assets, systems and networks would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof.

Exhibit 2

DHS considers power generation part of the energy industry, a critical infrastructure sector

US Department of Homeland Security's 16 designated critical infrastructure sectors

Department of Homeland Security Designated Critical Infrastructure Sectors	
1. Chemicals	9. Financial Services
2. Commercial Facilities	10. Food and Agriculture
3. Communications	11. Government Facilities
4. Critical Manufacturing	12. Healthcare & Public Health
5. Dams	13. Information Technology
6. Defense Industrial Base	14. Nuclear Reactors, Materials, and Waste
7. Emergency Services	15. Transportation Systems
8. Energy	16. Water and Wastewater Systems

Source: US Department of Homeland Security

The TSA has oversight of cybersecurity standards in six other sectors in addition to interstate pipelines: aviation, highway and motor carriers, maritime, mass transit and passenger rail, freight rail, and postal and shipping. Despite employing more than 50,000 people,

the department has the equivalent of only six full-time employees tasked with supervising the entire US interstate pipeline industry, which includes natural gas transmission pipelines, as well as pipelines transporting oil and other hazardous liquids. Furthermore, according to February 2019 testimony from Sonja Proctor, director of the Surface Division for the TSA's Office of Security Policy and Industry Engagement, none of the six employees have cybersecurity backgrounds.

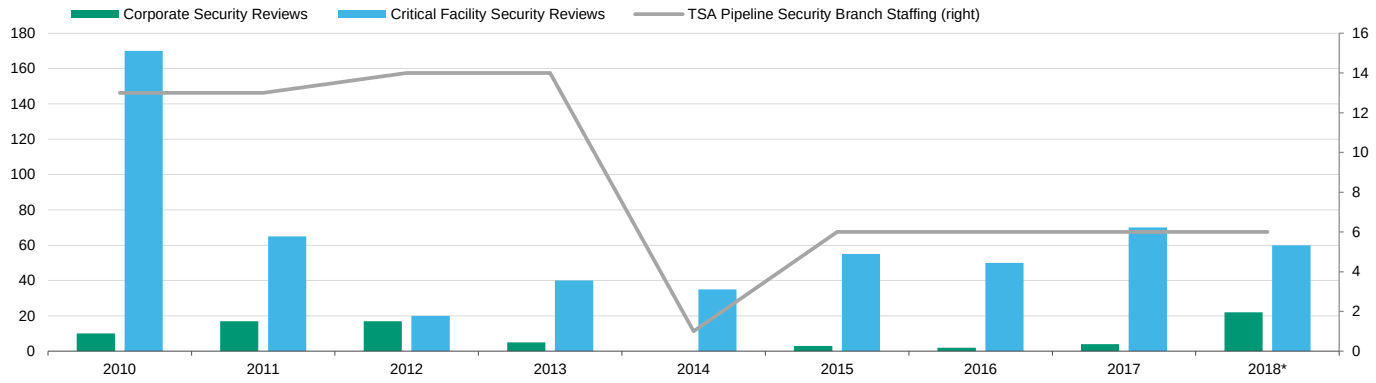
Among their responsibilities, TSA pipeline security employees are responsible for conducting security reviews of the pipelines they oversee. These reviews, which are voluntary, assess the extent to which the 100 most critical pipeline systems, identified based on the volume of natural gas they transport each year, follow the intent of the TSA's pipeline security guidelines.

The number of critical facility security reviews (i.e., on-site inspections of critical pipeline facilities and other select pipeline facilities), has fallen precipitously since 2010, despite the growing risk from attackers whose skill sets and tools have become more sophisticated. These reviews are more detailed than the TSA's corporate security reviews, which entail on-site inspections of a pipeline owner's corporate policies and procedures. As illustrated in Exhibit 3, the TSA completed only about 70 critical facility security reviews in 2017, the last full year of data available, down from over 160 in 2008.

Exhibit 3

Number of TSA critical facility security reviews has declined as risk of cyberattacks has grown

Annual number of TSA corporate security reviews and critical facility security reviews of transmission and distribution pipelines (left axis); number of employees in TSA pipeline security branch (right axis)



*Fiscal year 2018 data are through July 31, 2018

Source: Government Accountability Office

TSA officials say that staffing limitations within its pipeline security branch have prevented it from conducting more reviews. The decline in the number of reviews does not necessarily mean that natural gas pipelines have become more vulnerable to cyberattacks. But it does mean that the government has less visibility on the cyber defenses of an industry that it has identified as critical, which we view as credit negative.

That said, although improved government oversight of interstate pipelines would be a credit positive, the responsibility for protecting these assets from a cyber-attack ultimately lies with the operators' board of directors.

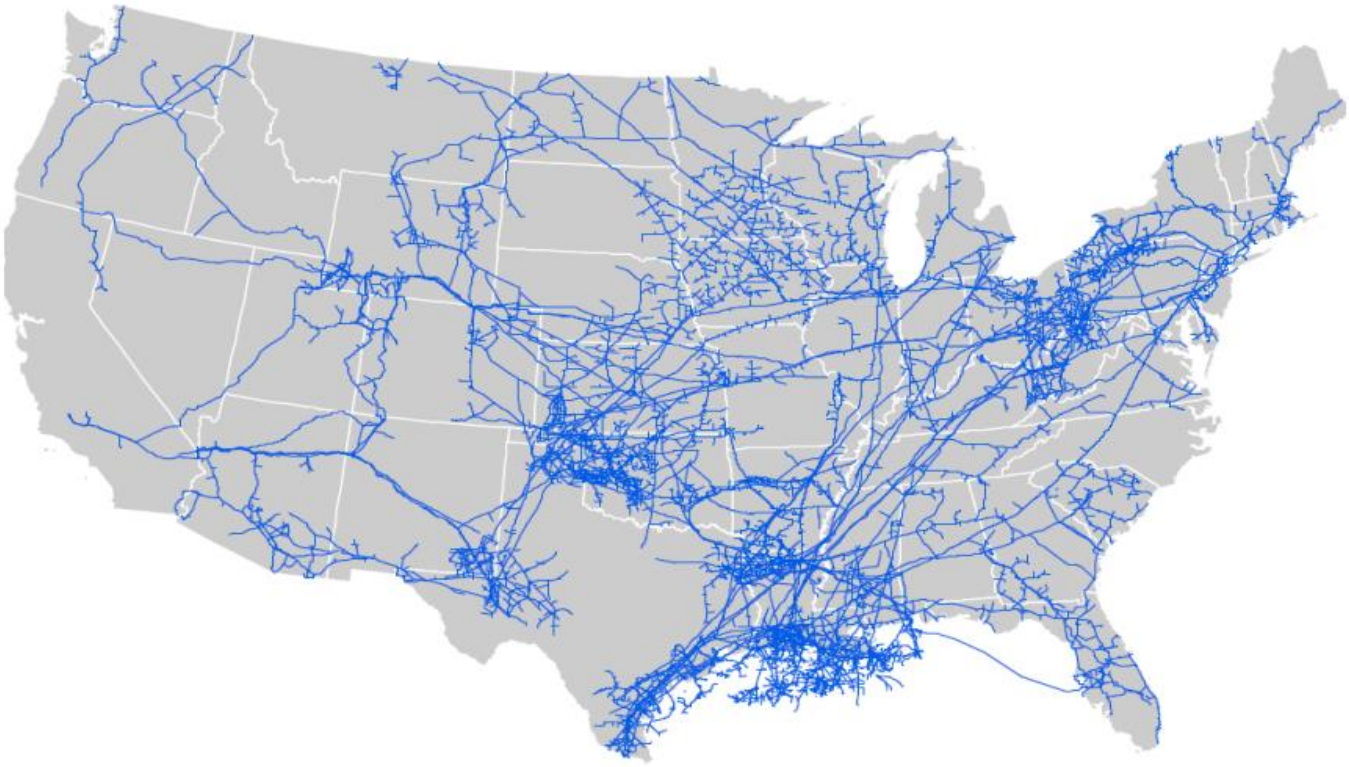
Natural gas pipelines are prized targets for cybercriminals

Natural gas has grown to become the largest fuel source for the US power generation sector, accounting for 34% of electricity generated in 2018. The interstate natural gas pipeline system is the key intermediary between the commodity's many suppliers and its users, utilities and independent power producers (see Exhibit 4). A disruption in the transport of natural gas could challenge the reliability of the affected area's electricity supply depending on the severity of the disruption and whether power generators in the affected areas have access to sufficient backup fuel sources.

Exhibit 4

Interstate natural gas pipelines transport the fuel powering over 30% of US electric generation

US interstate natural gas pipeline system



Source: U.S. Energy Information Administration

The increasing reliance of pipeline operators on sophisticated networked computerized systems and electronic data leaves them vulnerable to attacks from cybercriminals, who have identified natural gas pipelines as a prized target. Given the volatile and combustible nature of the product they deliver, as well as the potential consequences of a successful cyberattack, pipeline systems are attractive targets for hackers.

Operators are not currently required to report cyberattacks if they are not deemed material. As a result, complete data on the number and scale of attacks is not readily available. That said, the Department of Homeland Security began disclosing information about cyberattacks on the US pipeline infrastructure in 2012, when it revealed that an active "spear-phishing" campaign had targeted the US natural gas pipeline industry.

The federal government has continued to highlight these events since then. For instance, in March 2018, DHS and the Federal Bureau of Investigation reported that a nation-state had targeted organizations in the energy sectors and collected information about their industrial control systems. Industrial control system is a general term used to describe the integration of hardware and software with network connectivity to support critical infrastructure.

Attacks against industrial control systems have rapidly increased in sophistication as attackers' knowledge and capabilities have grown. Earlier this month, Dragos, a leading industrial control systems cybersecurity firm, called attention to the increased level of activity of XENOTIME, a group that seeks to compromise and disrupt industrial safety instrumented systems, with a particular focus on the oil and gas and electric sectors. XENOTIME rose to prominence in late 2017 after being identified as the group behind the TRISIS malware attack targeting Schneider Electric SE's (Baa1 positive) Triconex safety instrumented system. The multi-step malware framework caused industrial systems in a Middle Eastern industrial facility to shut down. According to Dragos, the incident represented an escalation in the capabilities and consequences of malware aimed at industrial control systems.

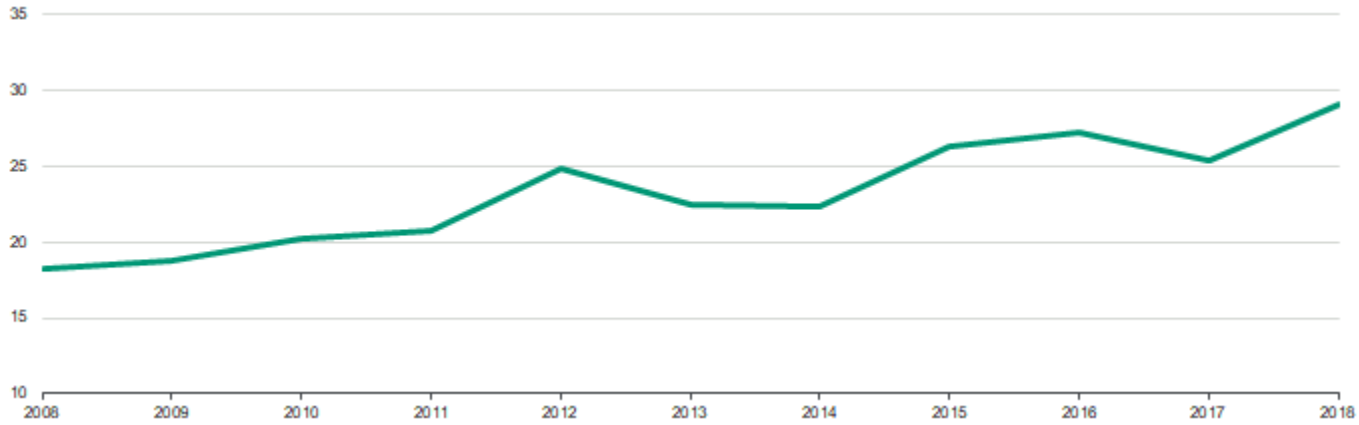
Interdependence between utilities and interstate natural gas pipelines is increasing

The confluence of the shale revolution started in 2008 and environmental concerns that have led to the retirement of coal plants has contributed to the emergence of natural gas-fired power plants as the most significant power generation source in the US. As shown in Exhibit 5, demand for natural gas among electric utilities has surged from about 18 billion cubic feet (bcf) in 2008 to nearly 30 billion cubic feet (bcf) in 2018. While the US Energy Information Administration expects demand growth to slow, natural gas power generation will continue to be the primary supplier of power for years to come.

Exhibit 5

Utilities' demand for natural gas to fuel power plants has nearly doubled in the last 10 years

Natural gas consumption by US electric utilities in billions of cubic feet



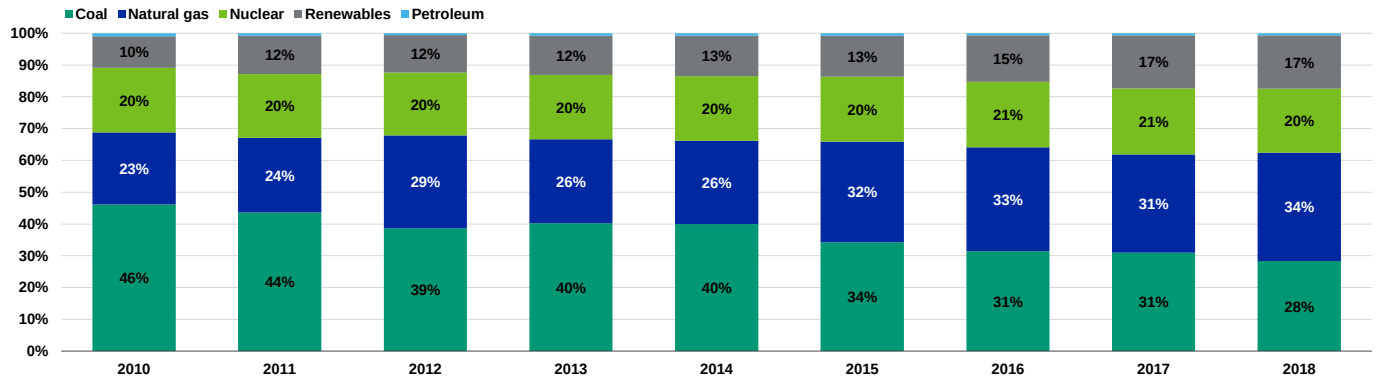
Source: U.S. Energy Information Administration

As shown in Exhibit 6, natural gas has accounted for the largest share of US power generation by fuel type since 2016. Looking ahead, we expect demand growth to slow, but natural gas power generation will continue to be the primary supplier of power for years to come as future retired coal-fired generating capacity will be replaced by a mix of new gas plants and renewables.

Exhibit 6

Natural gas became the primary source of fuel to the US power generation fleet in 2016

Share of annual power generation by fuel type



Source: U.S. Energy Information Administration

Moody's related publications

Sector In-Depth

» Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019

» Electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high, September 2018

» Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks, June 2017

» Cross-Sector - Global: Cyber risk of growing importance to credit analysis, November 2015

Sector Comments

» Utilities Remain Vulnerable and Attractive Target of Cyber Attacks, a Credit Negative, January 2017

» US Regulator Approves Cybersecurity Standards, a Credit Positive for Regulated Utilities, January 2016

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 1182252

MOODY'S
INVESTORS SERVICE