UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Security Investments for Energy Infrastructure Technical Conference	))	Docket No. AD19-12-000

COMMENTS OF THE AMERICAN GAS ASSOCIATION

Pursuant to the "Notice Inviting Post-Technical Conference Comments" issued by the Federal Energy Regulatory Commission ("Commission") on April 25, 2019, in Docket No. AD19-12-000, *Security Investments for Energy Infrastructure Technical Conference*,[1] the American Gas Association ("AGA") respectfully submits these comments. AGA appreciates the Commission and the United States Department of Energy ("DOE") holding a technical conference to discuss current cyber and physical security practices used to protect energy infrastructure and how federal and state authorities can facilitate security investments applicable to energy infrastructure, including the natural gas sector. As discussed in more detail below, AGA's comments focus on security matters related to the natural gas system in the United States, and particularly physical and cybersecurity issues facing natural gas local distribution companies.

[1] *Security Investments for Energy Infrastructure Technical Conference*, 84 Fed. Reg. 11777 (March 28, 2019) ("Notice").

I. COMMUNICATIONS

All pleadings, correspondence and other communications filed in this proceeding should be addressed to:

Matthew J. Agen
Assistant General Counsel
400 North Capitol Street, NW
Washington, DC 20001
(202) 824-7090
magen@aga.org

Michaela Burroughs
Senior Legal and Policy Analyst
400 North Capitol Street, NW
Washington, DC 20001
(202) 824-7311
mburroughs@aga.org

II. IDENTITY AND INTERESTS

The American Gas Association, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 74 million residential, commercial and industrial natural gas customers in the United States, of which 95 percent — more than 71 million customers — receive their gas from AGA members. AGA is an advocate for natural gas utility companies and their customers and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international natural gas companies and industry associates. Today, natural gas meets more than one-fourth of the United States' energy needs.[2]

AGA member companies take service from virtually every interstate natural gas pipeline company regulated by the Commission under the Natural Gas Act ("NGA"). As such, AGA members have an interest in the rates, terms and conditions of service provided by interstate pipelines, including policies and regulations affecting reliability and security. AGA and its operators implement security programs and actively engage in voluntary actions to help enhance the physical and cybersecurity of the nation's 2.5 million miles of natural gas pipeline and

[2] For more information, please visit www.aga.org.

distribution infrastructure, which span all 50 states with diverse geographic and operating conditions. AGA's members, therefore, have a direct and substantial interest in the issues raised in this proceeding.

III. COMMENTS

A. STATE AND FEDERAL ENTITIES HAVE A VESTED INTEREST IN FACILITATING ENERGY INFRASTRUCTURE SECURITY INVESTMENTS

Government and private entity partnerships are critical for effective cybersecurity management. America's natural gas delivery system is one of the safest, most reliable energy delivery systems in the world. Industry operators, however, recognize the inherent cyber vulnerabilities associated with employing web-based applications for industrial control and business operating systems. To address these vulnerabilities, natural gas utilities adhere to a myriad of physical and cybersecurity standards and participate in an array of government and industry cybersecurity initiatives. One of the most important protection mechanisms available to natural gas utilities is the existing cybersecurity partnership between the state and federal governments and industry operators. These partnerships foster the exchange of vital cybersecurity information, which helps stakeholders adapt quickly to dynamic cybersecurity risks. AGA and its members recognize the importance of this partnership and are committed to proactively collaborating with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving the security posture of natural gas local distribution companies and the industry's longstanding record of providing safe and reliable natural gas service across America.

1. STATE UTILITY COMMISSIONS ARE VALUED PARTNERS IN ENSURING THAT PROPER SECURITY MEASURES ARE IMPLEMENTED, AND EDUCATION IS ESSENTIAL TO SUCH PARTNERSHIPS

The various states and public utility commissions have a vested interest in encouraging and supporting physical and cybersecurity investments by natural gas utilities because such investments ensure safe and reliable natural gas service. State regulators and public utility commissions are charged with ensuring customers receive safe and reliable natural gas utility service at reasonable rates, among other responsibilities. Therefore, state and public utility commissions are valued partners with natural gas utilities in implementing proper physical and cybersecurity investments. While state regulators and public utility commissions are already hard at work to address cybersecurity risks, there is more to be done. This effort faces challenges in light of competing priorities for budget resources, a fluctuating workforce, and the need to navigate various requirements, which leads to state regulators seeking dynamic strategies to strike the right balance of potential risks, security, and available resources.

Education regarding potential physical and cybersecurity risks is an essential element of striking this balance. Natural gas utility companies work closely with their state regulators and public utility commissions to inform them of the physical and cybersecurity risks that the natural gas utility companies are facing. In addition to individual utility company efforts, the National Association of Regulatory Utility Commissioners ("NARUC") has historically been, and continues to be, effective in educating state public utility commission members and staff about physical and cybersecurity matters. One valuable tool used by NARUC to educate and promote a discussion on cybersecurity issues is NARUC's "Cybersecurity - A Primer for State Utility

Regulators" ("Primer").[3] The Primer was prepared by NARUC as a tool for policymakers that are charged with making decisions about the electric, gas, water, communications, and transportation systems that are vital to everyday life. Increasingly, utility systems are becoming more interconnected and more data is shared across systems. These capacities introduce cyber-vulnerabilities that must be managed by operators in partnership with applicable state commissions. As the Primer indicates: the regulatory role in cybersecurity is increasing; the number of cyberattacks to business processes is growing; and certain industry standards are driving new cybersecurity expenditures by utilities that may be featured in future rate cases.

Due to the ever-changing risk landscape, AGA is supportive of educational efforts on security as a way to ensure that state regulators and public utility commissions are informed of the possible physical and cybersecurity risks and also understand the motivations of natural gas utility companies seeking cost recovery for certain security initiatives. Further, efforts such as the technical conference held in this proceeding and efforts by NARUC help ensure that state commissions and federal agencies are valued partners in implementing security measures.

2. STATE AND LOCAL REQUIREMENTS PLACE DIFFERING RESPONSIBILITIES ON UTILITIES

Cybersecurity and physical security requirements and expectations are generally state specific with respect to risk assessment and prioritization of the natural gas utility company. Specifically, natural gas utilities are required by various statutes and tariffs to ensure essential human needs are served and address the priority levels in cases of service curtailment. These requirements, and the specifics of prioritization, may not be consistent with federal policy or

[3] *See* "Cybersecurity - A Primer for State Utility Regulators," last update in 2017, available at https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F. The current Primer focuses primarily on the electric sector, but the next update is anticipated to provide general concepts of how the Primer applies directly to the natural gas industry.

fully understood by different federal agencies and certain stakeholders. State regulators and natural gas utility companies are in the best position to understand regional or state specific service requirements. Therefore, AGA recommends that the Commission and DOE recognize that facilitating energy infrastructure security investments and evaluating a utility's security plans are not a one-size-fits-all endeavor. Each utility's physical and cybersecurity investments and related plans must be evaluated in the context of the relevant local and state service requirements which influence how a company guards against and responds to an incident.

3. INAPPROPRIATE RELEASE OF SECURITY INFORMATION SHOULD BE PENALIZED

One common area of focus for the Commission, DOE, and state regulators should be incentives to protect against, and the establishment of punitive penalties for, individuals that release protected security information. Penalties should be enhanced on state or federal government representatives, employees, or agents that publicly share protected security information or put such information at risk, regardless of whether the sharing is intentional or in error. AGA is concerned about having sensitive cybersecurity information inappropriately released to the public.

This is not a hypothetical concern; in late 2016, certain cybersecurity information about a Vermont electric utility was leaked to the press and erroneously reported on.[4] The report claimed that Russian hackers had penetrated the electric grid; however, this turned out not to be the case. The source for the story was information relevant to the industry, gathered by the intelligence community, and shared in an actionable and timely way between the utility and the government. Regretfully, the sensitive information was inappropriately released by a

[4] *See* "What electric utilities can learn from the Vermont hacking scare," Utility Dive, Jan. 10, 2017, available at https://www.utilitydive.com/news/what-electric-utilities-can-learn-from-the-vermont-hacking-scare/433426/.

government representative, who had inadvertently received the information when it was circulated to various government agencies.

A high level of trust *must* exist between utilities and regulators/governmental representatives, especially regarding issues of security, and there must be a confidential manner to report and discuss security risks and developments. Furthermore, there must be a manner to penalize those persons that wantonly or accidentally release such information. The inappropriate release of such information disincentivizes the sharing of threats, risks, and attack data, which would not be beneficial to the industry or its government partners.

B. FURTHER COORDINATION IS NEEDED BETWEEN THE VARIOUS AGENCIES THAT OVERSEE SECURITY

1. COORDINATION AMONG FEDERAL AGENCIES

While DOE has committed to taking additional steps to increase coordination, presently, there is inconsistent coordination between the various federal entities with an interest in energy security. This lack of coordination, for example, negatively impacts the exercises and programs developed to evaluate cybersecurity threats of the subsectors (oil, natural gas, and electric) of the energy sector. Since many federal and state regulatory agencies are involved in security activities, AGA suggests that the Commission share its operational insights with the government agencies tasked with overseeing natural gas pipeline infrastructure security and receiving the threat information from the field via the Energy Government Coordinating Council, which includes the Department of Homeland Security, DOE, and TSA, among others.[5] In the process, the Commission and its staff could inform voluntary guideline revisions or additions intended to increase security and share best practice recommendations. Further, the Commission should

[5] *See Energy Sector Government Coordinating Council Charter* (November 2014), *available at:* https://www.dhs.gov/sites/default/files/publications/Energy-GCC-Charter-2014-508.pdf.

provide subject matter expertise to existing authorities overseeing natural gas pipeline infrastructure security, including the Pipeline Hazardous Materials and Safety Administration, TSA, and DOE.

Further, AGA advocates for continued best practice recommendations and voluntary guidelines rather than for the creation of a strict rule-based regulatory structure for three reasons. First, cybersecurity, and the risks related thereto, are evolving quickly, making it challenging to know whether the response developed today to a security threat will remain viable a week or year from today. Since the process of standard development is so time-consuming and assumes a "one-size-fits-all" rule, it is not appropriate for an ever-evolving risk to installed systems. Second, not every natural gas utility system is the same, and voluntary guidelines, as opposed to a strict rule-based structure, supports smart, cost-effective solutions. For example, some natural gas utilities have installed dedicated microwave systems for supervisory control and data acquisition ("SCADA") purposes. Although costlier than alternatives, these systems may be considered an appropriate upgrade in certain service territories with large critical markets and appropriate terrain as opposed to smaller systems in isolated areas or difficult terrain. Other less costly alternatives may provide adequate protections in different and certain unique circumstances. Third, every company should remain actively involved in assessing security risk to its own infrastructure. A strict rule-based regulatory system would provide no incentive for continued active vigilance and could evolve into a system of passive rule compliance.

Additionally, AGA posits that the Commission, or any other standard-setting body, does not need to develop voluntary cybersecurity standards. The National Institute of Standards and Technology ("NIST") already provides guidance that can be adapted for each individual organization's risk framework and serve as a basis for that entity's best

practices for its unique operations. Furthermore, TSA provides existing pipeline security oversight and audits of critical infrastructure facilities as a function of its partnership with industry.[6] Furthermore, there are third-party firms that audit operations for compliance with governmental guidance.

2. COORDINATION AMONG FEDERAL AND STATE AUTHORITIES

Federal government representatives need to coordinate and communicate more with the various states when it comes to physical and cybersecurity and the natural gas industry. AGA recommends that federal policy-makers gain an improved understanding of, and respect for, the different types of energy delivery requirements/expectations state governments place on the natural gas utility companies within their jurisdiction. Similarly, states need to continue to engage with the natural gas utility companies and the federal government on security activities. Federal and state government entities should also continue to seize opportunities, such as the technical conference held in this proceeding, to learn more about the differences between the natural gas and electric systems, both from an operational standpoint and a security perspective. The similarities and distinctions between the two systems highlight the impact an incident might have and the level of resilience in each sector.

For example, the natural gas and electric utilities take seriously the responsibility to protect critical infrastructure, provide reliable energy for society and safeguard public safety and the environment. Both industries have adopted digital technologies to improve the reliability,

[6] Based on the Government Accountability Office's ("GAO") findings in its December 2018 report on Critical Infrastructure Protection, GAO-19-48, AGA is actively working with Congress to appropriately increase TSA pipeline security resources, particularly trained and capable staff necessary to conduct security reviews, perform trend analysis of data collected from security reviews, and assist with program management. Overall, providing additional personnel within TSA's pipeline security operation will benefit the industry's cybersecurity posture, bolster the industry's security partnership with the government, protect the public, and support TSA's mission to protection the nation's pipeline infrastructure.

efficiency, and the speed of operations and processes, such as industrial control systems ("ICS") which monitor and control physical assets. These systems include SCADA, process control networks ("PCN"), and distributed control systems. Both the natural gas and electric industries recognize the common significance of robust cybersecurity management of ICS.

However, there are fundamental differences between how the natural gas and electric industries transport the applicable commodity and operate their systems, and it benefits all stakeholders, in particular the government, to understand these differences and the corresponding different policy approaches for each. The inherent characteristics of natural gas are an important factor for reliability and resilience. Natural gas moves by pressure through a transportation system with the use of compressors that pressurize the gas to move it over distance. For long distances, compressors are placed at regular intervals to continue the forward movement. Since natural gas physically moves slowly through a pipeline at an average speed of 15-20 miles per hour, its flow can be controlled. This allows time for pipeline operators to manage the flow of natural gas and to adjust their operations in the unlikely event of a disruption. Additionally, natural gas production comes from diverse geographic supply areas spread across many U.S. states and Canada which contributes to ensuring that overall natural gas production is rarely affected by isolated local or regional events. The inherent operational nature of the natural gas system highlights the resilience of pipeline-transported natural gas, and the characteristics of natural gas distinguish it from the often more binary on/off nature of the electricity system. Both the similarities and differences between the natural gas and electric systems must be fully understood by the various federal agencies because the characteristics directly impact the risks to the systems and how best to respond.

C. FEDERAL STANDARDS OR GUIDELINES THAT DESIGNATE AN ENERGY FACILITY AS HIGH-RISK OR CRITICAL MAY CREATE CERTAIN CHALLENGES

The issue has been raised in this proceeding as to whether establishing guidelines or standards for high-risk or critical energy facilities, such as Defense Critical Electric Infrastructure,[7] is a way to incentivize prioritization of certain security investments. There are certain challenges to establishing guidelines or standards for high-risk or critical energy facilities as a way to incentivize a company to prioritizes certain security investments. First, there is a disconnect between what state and federal governments view as critical and high-risk and why such facilities are designated as such. Further, operators may view criticality as more dynamic, *i.e.*, a product of seasonality or system redundancy. Second, timely cost recovery that is limited to mandatory guidelines or standards for high-risk or critical energy facilities penalizes forward-thinking operators that are being proactive voluntarily and looking ahead to the next challenge related to its various facilities. AGA, therefore, does not recommend the establishment of federal guidelines or standards for high-risk or critical energy facilities, until the aforementioned issues are resolved.

D. FINANCIAL AND/OR ACCOUNTING INCENTIVES SHOULD BE CONSIDERED FOR PRUDENT CYBERSECURITY INVESTMENTS

AGA recommends that regulators and governmental authorities consider financial and/or accounting incentives for cybersecurity investments. Prudent cybersecurity investments in infrastructure and processes that ensure regular 'life cycle refreshes' reduce cyber risks. Life cycle refreshes ensure a proactive approach is taken to replacing aging computers and other items used to provide service. Such refreshes will ensure that appropriate support systems are in place and, in addition, may increase productivity and efficiency while serving customers. While

[7] Federal Power Act § 215A, 16 U.S.C. § 824o-1 (2019).

a one-size-fits-all approach may not be appropriate, there are a few incentives that could apply across all of the energy sectors. Examples of the incentive programs that regulators and governmental authorities should consider are tax credits on security investments and security certifications. Tax credits would reduce the costs of making cybersecurity investments. Moreover, a certification that represents a high level of security backed by the government can be used to obtain lower insurance rates and premiums, as demonstrated by other regulatory regimes.[8]

E. STATES SHOULD ENSURE THAT COST RECOVERY OPTIONS EXIST FOR COSTS RELATED TO PARTICIPATING IN VOLUNTARY FEDERAL PROGRAMS AND OTHER EXPENDITURES RELATED TO ADDRESSING SECURITY THREATS

To address the significant risk to safe and reliable operations posed by physical and cybersecurity threats, natural gas utility companies are actively participating in industry groups to determine and implement the most effective defenses. Further, AGA members utilize a number of available security standards, models, guidelines, and information sharing resources, including, but not limited to: (1) NIST's Framework for Improving Critical Infrastructure Cybersecurity, (2) DOE's Cybersecurity Capability Maturity Model ("C2M2"), (3) Department of Homeland Security Industrial Control System Computer Emergency Readiness Team (ICSCERT), and (4) TSA's Pipeline Security Guidelines. Natural gas utility companies are aware of and are compliant with established standards and protocols. In the end, if a natural gas utility company can offer support demonstrating it is devoting sufficient resources to meeting these threats, cost recovery options should be available.[9]

[8] *See, e.g.*, Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002, 6 U.S.C. §§ 441-444 (2019).

[9] For example, cost recovery options should exist for utilities implementing cybersecurity measures as well as physical infrastructure facilities, such as advanced video surveillance, sensor technology, physical barriers, lighting,

Currently, states' rules around security riders vary, but certain natural gas utility companies can recover physical and cybersecurity investments prior to a full rate case.[10] However, a more conventional recovery model holds the natural gas utility company at risk for the costs associated with addressing physical and cybersecurity threats until the completion of the full rate case process. Allowing for riders based on, for example, the TSA Pipeline Security Guidelines,[11] NIST's Framework for Improving Critical Infrastructure Cybersecurity[12] or C2M2[13] could accelerate the adoption of enhanced security practices and tools.[14] Such approaches are uniquely valuable in the constantly morphing cyber threat landscape.

Additionally, technology is moving to cloud-based services, and in many cases, the cloud offers additional security measures not available on premise. The viability of such services remains in question for ICS and other critical operations. For non-critical functions and in general, cloud services have advantages but are predominately categorized as operations and maintenance ("O&M"), not capital. The current method for allowing regulated natural gas utility companies to only earn on capital is slowing the adoption of some of these enhanced services. Also, certain current recovery methods do not support natural gas utility company O&M expenditures on supplementary cybersecurity activities such as cyber mutual assistance programs and cyber response exercises with public-sector response assets.

---

fencing, *etc*., pursuant to the aforementioned security standards, models, and guidelines. *See, e.g.*, TSA's Pipeline Security Guidelines, Sections 6 and 7, regarding Facility Security Measures and Pipeline Cyber Asset Security Measures.

[10] *Compare* the Statement of Commissioner J. Emler, Kansas Corporation Commission in Docket No. AD19-12-000 and K.S.A. § 66-2202 (Kansas statute discussing how utilities are permitted to recover capital costs for security through a gas system reliability surcharge) *with* the Statement of President P. Kjellander, Idaho Public Utilities Commission in Docket No. AD19-12-000 ("Building cybersecurity costs into base rates is one of the most preferred approaches.").

[11] Available at https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

[12] Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[13] Available at https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0.

[14] These types of high-level standards could serve as a barometer of prudence for cost recovery, but the is not meant to be a complete list of reasonable or prudent activities.

Finally, the state commissions should recognize that capital investment in digital systems may have shorter than projected operational lifespan due to cybersecurity concerns. For example, being best-in-class 256-bit AES encryption of today may be totally outclassed by quantum computing ability to break encryption in 15 years, effectively halving the expected 30-year lifespan of a control system. For the reasons stated above, AGA recommends that states review current practices to ensure that recovery of prudent security related investments and eliminate regulatory barriers that may inhibit investment.[15]

F. FEDERAL AND STATE AUTHORITIES SHOULD NOT ATTEMPT TO PRIORITIZE SPECIFIC INCENTIVES FOR SECURITY INVESTMENTS

Addressing physical and cybersecurity threats are of the utmost importance to natural gas utilities. However, incentives that prioritize specific security investments or micromanage security efforts provide little benefit towards addressing such threats. Each energy infrastructure facility or system, each company, and each region of the Unites States is different. Therefore, the security risks and possible investments are unique for each company. While prioritization of some incentives might work and appeal to certain companies, those same incentives may not be desirable for other companies. Prioritization is best left to the individual natural gas utility companies.

AGA recommends that federal and state authorities continue to coordinate and converse with natural gas utility companies as to what is needed to address physical and cybersecurity threats on an ongoing basis. As part of this approach, federal and state authorities should remain

[15] Regarding interstate pipelines, AGA encourages pipelines to work individually with customers and the Commission to permit the timely recovery of infrastructure security costs that are important in safeguarding critical infrastructure.

technologically agnostic and not press one technology over another via a one-size-fits all incentive process.[16]

IV. CONCLUSION

Wherefore, the American Gas Association respectfully requests that the Commission consider these comments in this proceeding.

Respectfully submitted,

/s/ Matthew J. Agen

Kimberly Denbow
Senior Director
Security, Operations and Engineering Services
American Gas Association
400 North Capitol Street, NW
Washington, DC 20001
(202) 824-7334
kdenbow@aga.org

Matthew J. Agen
Assistant General Counsel
American Gas Association
400 North Capitol Street, NW
Washington, DC 20001
(202) 824-7090
magen@aga.org

Michaela Burroughs
Senior Legal and Policy Analyst
American Gas Association
400 North Capitol Street, NW
Washington, DC 20001
(202) 824-7311
mburroughs@aga.org

May 28, 2019

[16] If federal and state authorities determine it is necessary to incentivize certain security investments, AGA would recommend that governmental authorities prioritize incentives that are cross-functional with pipeline integrity investments. For example, the authorities could investigate incentivizing the addition of redundancies and manual valves, *etc.*, while operators are replacing facilities.