The Honorable Dave McCurdy
President and CEO
American Gas Association

Testimony before the Senate Committee on Energy & Natural Resources
"Protecting the U.S Energy Delivery Systems from Cyber Threats"

April 4, 2017

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, I am Dave McCurdy, President and CEO of the American Gas Association. Also relevant to this hearing, I am a former Chairman of the House Intelligence Committee and have been heavily involved in computer, software, and internet policy since before it was called "cybersecurity." Also relevant in my background, I served on the Board of the Software Engineering Institute and in 2001 co-founded the Internet Security Alliance, a partnership between the Electronic Industries Alliance and the CyLab at Carnegie Mellon University. Thank you for inviting me to share my perspectives on critical infrastructure cybersecurity.

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 72 million residential, commercial and industrial natural gas customers in the U.S., of which 94 percent — over 68 million customers — receive their gas from AGA members. Today, natural gas meets more than one-fourth of the United States' energy needs. Natural gas is the foundation fuel for a clean and secure energy future, providing benefits for the economy, our environment, and our energy security. Alongside the economic and environmental opportunity natural gas offers our country comes great responsibility to protect its distribution pipeline systems from cyberattacks.

Technological advances over the last 20 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected and more efficient industry is that we have become an attractive target for increasingly sophisticated cyber terrorists. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a successful ongoing cybersecurity partnership with the Federal government.

When this hearing is complete, I hope the committee will have a strong understanding of at least four critical realities related to energy sector cybersecurity generally and pipeline transportation security and cybersecurity specifically.

- **Industry Commitment**. Natural gas utilities and our partners across the energy sector – from the CEO level on down – are exceptionally aware of cyberthreats and the potential consequences of a successful cyber attack. This awareness requires us to be vigilant and drives us to employ the best systems and personnel available to protect our business and operating systems, but more importantly, the millions of customers we have a duty to serve.
- **Energy Sector Coordination**. The business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their customers; therefore, the continued availability of abundant and affordable natural gas supplies, and the safe and reliable transportation of such gas supplies is of primary importance to their businesses and their regulatory obligations to serve. It is thus critically important that policy discussions surrounding gas-electric interdependency/coordination, address the reliability of both the gas and electric systems in a coordinated manner.
- **Maintain Existing Security Partnerships.** Gas utilities maintain a longstanding and effective pipeline transportation security partnership with the Department of Homeland Security (DHS), specifically the Transportation Security Administration (TSA). The industry also works closely with the Department of Energy (DOE) on general energy sector physical and cybersecurity. These non-regulatory security partnerships are built on cooperation, mutual trust, and most importantly the recognition that a top-down cybersecurity regulatory regime would be counterproductive to industry security. Simply put, our adversaries move faster than any regulatory checklist so it's better to partner on protecting our systems than to rely on static compliance programs. Further, reshuffling our government cybersecurity partners will also not make us any safer. Granting DOE additional authority over pipeline transportation systems security virtually guarantees unnecessary program overlap with existing TSA programs. Shifting the entire pipeline transportation security regime from TSA to DOE ignores the pipeline expertise and industry knowledge TSA has built over a decade of partnership, a program that would have to be rebuilt at DOE.
- **Public-Private Collaboration**. The single most important aspect of cybersecurity policy remains effective government-private sector partnership. In order to better protect our systems, industry needs better cybersecurity information from our government partners delivered in real-time; quicker dissemination of classified threat information; and a closer working relationship with not only our sector specific agencies (TSA and DOE), but the law enforcement and intelligence community so we can leverage their unparalleled knowledge and capabilities. Finally, we need to reform the process by which industry leaders receive security clearances. [*A personal point of privilege: Despite my long history of service in the government intelligence space, and despite my existing Department of Defense security clearance, I still have not received a DOE security clearance. I applied well over a year ago*.]

COMMITMENT TO SECURITY

AGA member utility executives have signed onto the *AGA Commitment to Cyber and Physical Security* (Commitment) (see Appendix A), formally demonstrating their dedication to ensuring natural gas pipeline infrastructure remains resilient to the growing and dynamic cyber and physical security threats faced by the industry. The Commitment was developed at the direction of the AGA Board with full CEO support. As outlined in the Commitment, AGA member utilities are dedicated to proactively collaborating with Federal and State governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving their security posture and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

Security awareness is part of the natural gas utility culture and daily practice. The Commitment identifies a consensus by AGA members of actions and accompanying elements that help enhance the resilience of a company's gas operations to security threats. The Commitment further acknowledges that the method and timing of implementing such actions may vary with each operator, taking into consideration individual environments, identified risks, and what has been deemed reasonable and prudent by their state regulators or governing bodies. AGA member utilities recognize the significant role that state regulators or governing bodies play in supporting and funding these actions. As such, effective, performance-based implementation is beyond prescriptive, "check-the-box" compliance.

STRATEGY – REMAIN ON THE OFFENSIVE

Natural gas utilities and pipelines actively engage in cybersecurity risk management. Our primary objectives are to minimize cyber vulnerabilities and increase the natural gas operator's ability to detect malicious cyber traffic, mitigate potential impact, and implement security measures that ensure the safe and reliable delivery of natural gas to customers is not disrupted. Cybersecurity effectiveness in the natural gas industry is maximized by the diversity of protective measures industry-wide that achieve the same overall objectives.

In general, natural gas operators across the industry use the "resiliency in depth" strategy to protect their networks. This strategy begins with corporate cybersecurity governance consisting of policies, standards and guidelines designed to protect critical operations networks, which may include industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA). SCADA consists of software and hardware for system operations and may be applied differently across the industry. Some operators use SCADA only to monitor critical data from sensors, while others use SCADA additionally for system control. Basically, SCADA sends compiled data to a central computer for a human operator to analyze to determine if signals need to be sent out to control field equipment and pipeline conditions. The introduction of SCADA technology to natural gas operations significantly increased natural gas delivery efficiency, reliability, and safety. Industry operators recognize the application of ICS has inherent cyber vulnerabilities, and they identify, evaluate, and manage these risks accordingly. Natural gas utilities and pipelines apply a portfolio of tools, policies, procedures, and practices to manage cybersecurity vulnerabilities and stay ahead of threats. The ultimate objective: Remain on the offensive.

As the Committee knows, there is no single best practice for cybersecurity protections among natural gas utilities, let alone across the energy sector. More to the point, the diversity of operations and SCADA applications across the industry adds to overall sector security because there is no security benefit in identical operating environments. Operators implement security programs and actively engage in voluntary actions to help enhance the security of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions.

AGA members utilize a number of available security standards, models, guidelines, and information sharing resources (Appendix B), including, but not limited to: (1) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, (2) Department of Energy *Cybersecurity Capability Maturity Model* (C2M2), (3) Department of Homeland Security *Industrial Control System Computer Emergency Readiness Team* (ICS-CERT), (4) TSA *Pipeline Security Guidelines*, and (5) North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. Cybersecurity cannot effectively be treated as a static threat. As cybersecurity risks and threats change, so do vulnerabilities. As such, ongoing implementation of new tools and capabilities is vital to adapting to the dynamic cyber environment.

In addition, AGA gas utilities and transmission companies participate in the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC), enabling them to share real-time threat intelligence and pertinent information to help them keep their systems secure. Other information sharing entities in which AGA member utilities participate include State Fusion Centers, other ISACs (e.g., Electricity ISAC, Oil & Natural Gas ISAC, Multi-State ISAC, Financial ISAC, Industrial Control System ISAC), and cross-sector information sharing initiatives (e.g., TSA Alerts, USCYBERCOM, DOE Situational Awareness Reports, government intelligence community Joint Analysis Reports, Railway Alert Network, and the Interstate Natural Gas Association of America (INGAA) ThreatConnect program.

Beyond technology, standards, and tools, cybersecurity program effectiveness starts with employee training and awareness of cybersecurity risks and how they may be used by adversaries to gain unauthorized access to networks. Natural gas utilities dedicate substantial resources to reinforcing cybersecurity hygiene awareness at all levels of the corporate structure – from the field employee to the board room. Natural gas utilities also conduct social engineering penetration assessments of their employees to identify those individuals who may require increased cybersecurity awareness training.

FEDERAL & STATE GOVERNMENT ROLES

Pipeline Security Regulatory Authority

The *Aviation & Transportation Security Act of 2001* gave the Department of Homeland Security (DHS) security authority over all modes of transportation, including modes under the purview of the Department of Transportation. Specific to pipeline security, oversight was given to the Transportation Security Administration (TSA), and TSA has been partnering with natural gas

pipelines for over a dozen years. This partnership has been fostered by onsite audits conducted by TSA, conferences jointly sponsored by TSA and industry operators, open communication and exchange of smart practices, and voluntary sharing and analysis of emerging security challenges. Through a multi-year effort and comprehensive forums, TSA developed the *TSA Pipeline Security Guidelines* (Guidelines) in coordination with the pipeline industry. These Guidelines were released in late 2010 (re-released in 2011 to incorporate the National Terrorism Advisory System) and are presently under revision to address lessons-learned and ongoing changes to the cyber threat landscape. The Guidelines have been widely adopted by industry since initial completion in 2009. AGA member gas utilities implement these Guidelines as applicable to their individual environments.

TSA's strategic decision to partner with industry instead of regulate has created a constructive and open relationship with natural gas utility partners that has advanced security beyond a solely compliance mindset. Compliance does not equate to security, and TSA understands this. By working closely with industry for over a decade, TSA has a developed thorough understanding of pipeline operations. Additionally, TSA and the Department of Transportation (DOT) have a Memorandum of Understanding to coordinate pipeline safety and pipeline security, which further enhances TSA's role in coordinating and promoting security throughout the sector.

DHS Cyber Vulnerability Assessment of ONG Value Chain

In February 2013, Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," was issued. Per the requirement in Section 9, DHS conducted cyber vulnerability assessments of all the critical infrastructure sectors, including the Oil and Natural Gas (ONG) sector to identify U.S. cyber-dependent critical infrastructure "where a cyber incident could reasonably result in catastrophic regional or national effects." Based on an evaluation of the threats and the mechanisms in place that enhance ONG resilience, DHS concluded ONG did not belong on the Section 9(a) list.

In conducting the assessments, the ONG sector worked with DHS to identify business functions and associated value chains along the commodity path from well-head to end-user. Functions with a cyber-component, regardless of housing on the enterprise network or the operating network, were identified and a series of cyber-provoked scenarios were discussed along with how consequences would measure up to the criteria proposed by DHS.

From a cyber design perspective, natural gas functions are divided across an enterprise network (which handles emails, billing, invoices and basic corporate data and information) and an operations network (which includes control system, SCADA, and pipeline monitoring). These two networks are isolated from each other, employ firewalls and layer other tools and mechanisms to improve the prevention, detection and mitigation of cyber penetration. Further, the inherent design of high pressure and low pressure gas delivery systems is mechanical by nature. Modern infrastructure has control systems to help operate and monitor pipelines and pipeline components to move the product in a reliable, efficient and effective manner. Operators manage the internal pressure of the delivery system by controlling the amount of natural gas entering and leaving the system. The process of increasing or decreasing pressure happens

relatively slowly in a natural gas system because of the compressible nature of the gas. This compressibility lessens the immediacy of a potential cyber attack's impact and increases the probability of detection. Layered onto this control system architecture are mechanical overpressure protection devices, which serve as a safeguard to prevent internal gas pressure from threatening a pipeline's integrity. Pipeline safety regulations and standards require that back-up systems CANNOT be affected by the same incident that compromises the primary control system; thus, fail-safes and redundancies must be independent of the cause of the primary mechanism's failure.

Sector Specific Agencies

The Homeland Security Presidential Directive 7 (HSPD-7) of 2003 identified critical infrastructure sectors and Federal government agencies/offices to serve as Sector Specific Agencies (SSAs) responsible for implementing the National Infrastructure Protection Plan framework and guidance as tailored to the specific characteristics and risk landscapes of each sector to which the SSA is assigned. Natural gas utilities and pipelines fall under the purview of at least two SSAs, i.e., DHS TSA[1] as the SSA for pipelines (identified as a mode of transportation) and DOE as the SSA for energy. The DHS Office of Infrastructure Protection may be an additional SSA depending upon the business functions of the company.
In its role as the SSA for the Energy Sector, DOE has worked closely with government and industry partners to develop cybersecurity practices, tools, and guidelines that address relevant cybersecurity risks and threats. Much of this work has been and continues to be done in collaboration with the two Energy Subsector Coordinating Councils (SCCs) and the Energy Government Coordinating Council (GCC). The Electricity SCC and the Oil & Natural Gas SCC (ONG SCC) comprise the Energy SCCs and represent the interests of their respective industries. The Energy GCC represents government at various levels – Federal, State, local, territorial, and tribal. Through the partnership created under the NIPP framework, SCC and GCC partners work together towards the ultimate end-goal of protecting and securing the American energy system.

Other Federal government entities with pipeline cybersecurity interests and with which natural gas utilities and pipelines coordinate include the DHS Infrastructure Security Compliance Division, United States Coast Guard, and the Federal Energy Regulatory Commission. Additionally, natural gas utilities and intrastate pipelines are subject to State government actions.

PROACTIVE INITIATIVES

Natural gas utility security challenges, like the threat environment in which they operate, are constantly changing. To address these challenges and to predict future challenges, AGA and its member utilities have an array of strategically planned initiatives to educate, coordinate, and motivate industry resilience. Leading challenges include sector interdependencies, supply chain integrity, Internet of Things, and the convergence of physical and cybersecurity. Initiatives

[1] The Department of Transportation and DHS are directed by HSPD7 to collaborate on all matters relating to transportation security and transportation infrastructure protection.

include partnering within the Energy Sector, with other interdependent sectors, and with government partners. Programs already referenced include development of the DNG ISAC and the *Commitment to Cyber & Physical Security*. Additional initiatives include active engagement with the revisions to the *TSA Pipeline Security Guidelines* and to the *NIST Cybersecurity Framework*, Downstream Energy Coordination, educational activities with State regulators, assistance with industry-wide implementation of the DOE ONG C2M2, identification of leading cybersecurity threats to natural gas utilities, topical workshops, cybersecurity tabletop exercises, and senior executive engagement. Details for each follow.

- **AGA Commitment to Cyber and Physical Security:** The *AGA Commitment to Cyber and Physical Security* (Commitment), which was approved by the AGA Board in October, 2016, outlines industry's continued commitment to improving security through voluntary actions and closely aligns with the *TSA Pipeline Security Guidelines (2011)* and the *NIST Cybersecurity Framework (2014)*. The Commitment demonstrates to interested stakeholders that industry is voluntarily taking actions to identify, protect, detect, respond, and recover from a physical or cybersecurity attack. At the direction of the AGA Board, AGA has moved forward with collecting letters of commitment from AGA member company executives. AGA has been commended by DHS, DOE, TSA, and DOT for this effort.
- **Downstream Natural Gas Information & Analysis Center (DNG ISAC):** The DNG-ISAC supports natural gas operators with cyber and physical security alerts of greatest relevance to natural gas operations. Participation includes AGA member gas utilities, the Canadian Gas Association, and the Interstate Natural Gas Association of America. This provides all natural gas distribution and transmission companies in the U.S. and Canada unfettered access to real time actionable information, security alerts, and analysis to enable them to better secure their cyber and physical assets.
- **Updating 2011 Transportation Security Administration (TSA) Pipeline Security Guidelines.** The *2011 TSA Pipeline Security Guidelines* (Guidelines) is a collaboration of TSA, pipeline operators (including AGA), and other government entities with an interest in pipeline security. It has been five years since the release of the Guidelines, and TSA and stakeholders are once again partnering to review and ensure the Guidelines are up to date and an effective pipeline operator security resource.
- **NIST Cybersecurity Framework.** Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directed the National Institute of Standards & Technology (NIST) to develop a cybersecurity framework applicable to all 16 critical infrastructure sectors. Natural gas utilities and pipelines committed to the collaborative development of this framework. Released in February 2014, the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) is essentially a maturity model intended for voluntary adoption by critical infrastructure owner/operators. Additionally, DOE and industry partners (including ONG) collaborated to develop the *Energy Sector Cybersecurity Framework Implementation Guidance*, which relies on existing sector-specific standards, tools, and processes to help industry characterize, enhance, and communicate their cybersecurity posture using the NIST Cybersecurity Framework. TSA collaborated similarly with sector partners (including pipelines) to develop the *Transportation Systems Sector Cybersecurity Framework Implementation Guidance.* In January, 2017 NIST released

an updated Cybersecurity Framework and pipelines are once again engaged to ensure the revisions build upon the current wide-spread acceptance and adoption of the Cybersecurity Framework.

- **Downstream Energy Coordination.** AGA leads the downstream energy coordination initiative on behalf of the ONG SCC in partnership with the ESCC. Oversight is provided by a prominent gas/electric utility CEO. This initiative focuses on the interdependency of natural gas and electric utilities to plan for and respond to major incidents, better understand and protect mutual dependencies, share information, and improve cross-sector situational awareness. This coordination has led to opportunities for cross-subsector education and information exchange to the benefit of government and industry stakeholders.
- **Activity with States.** Recognizing the significant role state regulators or governing bodies play in supporting and funding of cybersecurity actions of natural gas utilities, industry operators are engaging with State-level leadership. The National Association of Regulatory Utility Commissions (NARUC) developed a reference guide, "Cybersecurity for State Regulators," a primer that explains cybersecurity basics and includes questions State regulators and utilities may use to engage in partnerships. AGA encourages gas utilities to use this primer to reach out to State regulators.
- **Regional Cybersecurity Assessment Workshop.** AGA is in its third year of sponsoring regional cybersecurity assessment workshops with the objective of assisting member companies with evaluating the maturity of their cybersecurity programs through facilitated application of the DOE ONG Cybersecurity Capability Maturity Model (ONG C2M2). Participating companies leave the workshop with an assessment of their overall corporate cybersecurity capabilities and identified areas for further consideration and planning.
- **Cyber Threat Analysis Guidance.** The AGA Cyber Threat Analysis initiative identified leading cybersecurity threats to natural gas utilities; developed a resource tool detailing each threat, associated threat vectors, consequences, threat elements, and mitigation measures; and culminated in a workshop that brought together cyber and operations professionals representing three dozen natural gas companies to discuss the potential impact of these threats on their companies' operations infrastructure.
- **Topical Workshops & Tabletop Exercises.** AGA continues to present timely, well-attended topical workshops on areas of interest and opportunity for advancing natural gas utility cybersecurity programs. Recent workshops include *Cyber Risk Taxonomy*, *ONG C2M2 Lessons Learned*, *Shodan & Metasploit Overview*, and *Insider Threat*. AGA also hosts multi-dimensional tabletop exercises that touch on a variety of business functions upon which natural gas operations rely, including gas control, operations, telecommunications, cyber, physical security, and electricity. The last exercise scenario was developed with input from DHS ICS-CERT and the DOE Idaho National Laboratory.
- **Senior Executive Engagement.** Biennially, AGA presents the *Energy Delivery Cybersecurity Executive Summit* bringing together leading executives from across the Nation with a stake in natural gas energy delivery, including electric, oil, telecommunications, and finance. The objective of the Summit is to engage government and private sector leaders to discuss cyber interdependencies, increase awareness of shared

vulnerabilities, and continue our commitment to effective, coordinated strategies. The 2017 event will be co-sponsored by the Canadian Gas Association and held in conjunction with *NERC GridEx IV* to maximize cross-border and cross-sector coordination.

NATURAL GAS & ELECTRIC POWER GENERATION INTERDEPENDENCY

The growing interdependencies between the natural gas and electricity subsectors are well-recognized. The increased use of natural gas for power generation is due to many factors, including – environmental regulations, abundant and affordable fuel, and significant increase in domestic production. This interdependency has effectively expanded the customer base of our nation's natural gas delivery portfolio that has required a new level of physical, operational, legal, and regulatory understanding between the two industries. The natural gas and electric industries have been working together to increase the understanding of each other and to address challenges by increasing coordination and communication regarding understanding the natural gas value chain, natural gas contractual obligations, physical natural gas system operations and limitations, natural gas limiting regulations, natural gas emergency service priority requirements,[2] and the need to coordinate cybersecurity resiliency efforts.

America's natural gas production, transmission, storage, and distribution systems support the most flexible and resilient natural gas market in the world. The U.S. pipeline and storage network is highly reliable, the result of accessible production from virtually all major North American gas producing regions and delivery via an integrated pipeline transportation network. The business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their direct-use customers.[3] Therefore, the continued availability of abundant and affordable natural gas supplies, and the safe and reliable transportation of such gas supplies is of primary importance to their businesses and their regulatory obligations to serve. It is thus critically important that discussions surrounding gas-electric interdependency, as well as our national policy, address the reliability and resiliency of both the gas and electric systems, while recognizing the differences between the industries.

Reliability of natural gas service and system resiliency is a priority for both the natural gas and electric industries. This is particularly important for natural gas utilities because they have state regulatory mandates or obligations to serve firm, or core, customers (generally residential and small commercial) which requires them to reliably meet the natural gas supply needs of these customers at just and reasonable rates, terms and conditions of service. To fulfill this public service obligation, gas utilities develop comprehensive plans and manage assets, operations and contractual portfolios that include physical natural gas supply arrangements, natural gas transportation, and natural gas storage. Natural gas utilities plan their supply portfolios and build their system deliverability to ensure reliable service to these firm customers and others on a

[2] For gas-fired generators located on natural gas utility systems, it is important to note that gas curtailment priorities are state-specific determinations. For gas-fired generators served directly off an interstate pipeline, there are interstate pipeline tariff provisions that set forth transportation service priorities.

[3] Not discussed in depth here, natural gas pipelines also are subject to pipeline safety regulations, which address the resilience and reliability of the pipeline infrastructure.

"design day" (or a forecasted peak day load based on historical weather conditions). The methodologies for design day determination vary among gas utilities, but are based typically upon the principle of maintaining service to these firm customers on the coldest days of winter.

Through this planning, natural gas utilities build systems and enter into contractual arrangements seeking to ensure continuous gas service operations throughout each year. Planning includes contingencies to address physical operational service disruptions in various scenarios, as well as other circumstances, such as extreme weather events and planning system resiliency against cyber threats – all of which may impact or disrupt natural gas service. An important component for gas service reliability regards the planning and development of needed infrastructure. Adequate and reliable infrastructure is a critical component of a healthy and liquid natural gas market. As more power generation moves to the use of natural gas for fuel, certain regions of the country, particularly the Northeast, will need additional infrastructure to serve this new load. But each region of the country has a unique energy portfolio, and the timing of infrastructure development will be regionally-dependent.

Natural gas utilities also provide reliability by contracting at the highest level of service reliability offered by the pipeline – generally at a firm service level. While unusually severe weather events have the potential to disrupt the natural gas system, the loss of pipeline transportation and storage services that are contracted for on a firm basis have been rare. During periods of high usage and system constraints, prevalent on the coldest winter days, natural gas systems may call upon customers that have contracted for lower priority services, such as interruptible service, to decrease or cease gas usage temporarily, upon which these customers generally have planned to switch to a back-up fuel, such as fuel oil. The tradeoff for these customers is a discounted rate for the natural gas delivery service, compared with firm service rates, and parties enter into these contractual arrangements with prior knowledge. To ensure reliability in periods of extreme weather constraints and other events, natural gas utilities routinely plan and contract for firm contracting levels for both natural gas commodity supplies as well as the transportation of such supplies on gas pipeline systems. Thus, if natural gas-fired power generators have decided to contract for interruptible transportation service on gas pipeline systems, they may find that interruptible transportation capacity is unavailable during severe weather or other outage events because the available pipeline capacity is being used by higher priority firm transportation service customers. In some circumstances, in order to provide additional firm services to customers, gas system operators may need to develop and construct additional infrastructure.

During coordination efforts to address the needs of the gas and electric industries, it has been emphasized that many gas services are offered and/or can be designed to help meet the needs of gas-fired generators. In seeking natural gas service reliability for their own circumstances, gas-fired power generators can learn from the natural gas utility planning and contracting model to assess their needs and pursue firm services as well as new or different services on gas pipeline systems that may not be currently available. In some cases, the provision of such services may require an appropriate expansion of natural gas infrastructure to meet the needs of gas-fired generation. However, AGA stresses that it is important that such gas services preserve reliability for all of the customers on the gas system and are aligned with the market

incentives for gas-fired generators to enter into contracts for those services, when needed, without the creation of cross-subsidies.

In considering the broad issues of how to achieve greater coordination between the natural gas and electricity markets, AGA believes that policies should be guided by the following principles:

- The overall goal of gas-electric coordination policies should be to preserve and, where appropriate, enhance reliability for all customers, both gas and electric:
- Gas and electric stakeholders must collaborate to meet this overall objective;
- Policymakers and industry leaders should ensure the policies they pursue address the reliability of both gas and electric systems in a coordinated manner, not one at the expense of the other;
- National policy cannot be made in isolation; there are a number of different considerations – including energy, environment, economics, national security and consumer interests;
- Policies should reflect variations in reliability issues at the regional level in terms of infrastructure, scope and timing. Priority should be given to those regions where the need is most urgent; and
- Policy initiatives should recognize ongoing regional efforts to address reliability issues, draw on stakeholders' existing knowledge of regional operations and promote continued collaboration among all stakeholders on a regional basis.

IN SUMMARY

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. Industry operators recognize the application of industrial control systems has inherent cyber vulnerabilities, and they identify, evaluate, and manage these risks accordingly. Security awareness is woven into the natural gas utility culture, and natural gas utilities and pipelines apply a portfolio of tools, policies, procedures, and practices to manage cybersecurity vulnerabilities and stay ahead of threats. Of these, the most important cybersecurity mechanism is the existing cybersecurity partnership between the Federal government and industry operators.

TSA, the regulator for pipeline security, has been partnering with the industry for over a dozen years. TSA's strategic decision to partner instead of regulate has created a constructive and open relationship with natural gas utility partners that has advanced security beyond a solely compliance mindset. Further, pipelines are subject to DOT pipeline safety regulations, which are intended to address the resilience and reliability of the pipeline infrastructure. Natural gas utilities' risk management takes into consideration upstream feeds, downstream customers, contractual agreements, and State service priority plans.

Building on the partnership model, natural gas utilities and pipelines work closely with its leading SSAs, i.e., TSA and DOE. In its role as the SSA for the Energy Sector, DOE actively engages with government and industry partners to develop cybersecurity practices, tools, and guidelines

that address relevant cybersecurity risks and threats. The partnership with DOE continues to be effective in identifying and solving constantly changing pipeline security challenges.

Additionally, AGA and its member utilities have an array of strategically planned initiatives to educate, coordinate, and motivate industry resilience through partnerships within the Energy Sector, with other sectors, and with government partners. This is particularly important given the growing interdependencies between the natural gas and electric industries, which has effectively expanded the customer base of our nation's natural gas delivery portfolio but not without accompanying challenges. The natural gas and electric industries have been working together to address such challenges, and more remains to be done. Given that the business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their customers, it is critically important that discussions that surround gas-electric interdependency/coordination as well as our national policy address the reliability of **both** the gas and electric systems in a holistic coordinated manner for the benefit of the energy consumer and our nation's economy.

Attached to this testimony are following additional supplemental materials:
1. AGA's Commitment to Cyber and Physical Security
2. Natural Gas Cybersecurity and Standards Portfolio

Thank you for the opportunity to provide this additional testimony for the record.

Respectfully submitted,

President and CEO
American Gas Association

AGA's Commitment to Cyber and Physical Security

AGA and its members are dedicated to help ensure that natural gas pipeline infrastructure remains resilient to growing and dynamic cyber and physical security threats. We are committed to proactively collaborating with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving our security posture and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

AGA and its operators implement security programs and actively engage in voluntary actions to help enhance the security of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions. The Department of Homeland Security Transportation Security Administration (TSA) has oversight for security of pipelines (including natural gas distribution and transmission), and as such, has developed the *TSA Pipeline Security Guidelines*. AGA member gas utilities and transmission companies are implementing these guidelines as applicable to their individual environments. Additionally, AGA members are utilizing a number of available security standards, models, guidelines, and information sharing resources, including, but not limited to: (1) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, (2) Department of Energy Cybersecurity Capability Maturity Model (C2M2), (3) Department of Homeland Security Industrial Control System Computer Emergency Readiness Team (ICS-CERT), (4) TSA Pipeline Security Smart Practices Observations, and (5) TSA Intermodal Security Training Exercise Program (I-STEP). In addition, AGA gas utilities and transmission companies will be part of the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) by 2017.

Below are voluntary security actions that are being taken by AGA or individual operators to help ensure the secure operation of natural gas pipeline infrastructure. AGA and its operators recognize the significant role state regulators or governing bodies play in supporting and funding these actions. It is the consensus of AGA members that the actions and accompanying elements listed below enhance the resilience of a company's gas operations to security threats. However, the method and timing of implementation of these actions will vary with each operator. Each operator evaluates, and implements as appropriate, these actions taking into account individual environments, identified risks, and what has been deemed reasonable and prudent by their state regulators or governing bodies.

IDENTIFY

1. Establish ownership, sponsorship, organizational roles and responsibilities for corporate security programs
2. Conduct criticality assessments to identify critical facilities
3. Identify critical cyber assets
4. Define security roles, responsibilities, and lines of communication
5. Intelligence gathering and information sharing

PROTECT

1. Review security plans and procedures
2. Implement access controls
3. Implement personnel training and awareness program(s)
4. Develop & implement maintenance program(s)
5. Incorporate security into system designs
6. Establish cybersecurity controls for procuring systems and services

DETECT

1. Implement intrusion detection and monitoring
2. Perform background investigations
3. Conduct periodic vulnerability assessments
4. Establish procedures for receiving and handling threat intelligence to improve detection capabilities

RESPOND/RECOVER

1. Develop communication procedures for security events
2. Conduct periodic drills and exercises
3. Plan and prepare for the restoration of systems, facilities, and assets
4. Establish redundancies for resilience
5. Establish procedures for responding to threat information and actual events

NATURAL GAS CYBERSECURITY GUIDELINES & STANDARDS PORTFOLIO

Gas utilities and transmission operators apply a myriad of cybersecurity standards, guidelines, and regulatory practices, and tools developed by industry and government entities in their cybersecurity portfolio, as applicable to their individual security environments. These include, but are not limited to:

- American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*
- *AGA Commitment to Cyber and Physical Security* (2016)
- *AGA Cybersecurity Procurement Language Tool*
- *AGA Report 12 – Part I, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*
- AGA and Interstate Natural Gas Association of America (INGAA), *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, (2008)
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-CDV3, *Enterprise-Control System Integration Part 1: Models and Terminology,* (2008)
- ANSI/ISA0-99.00.01-2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models,* (2007)
- ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- American Petroleum Institute (API) & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum & Petrochemical Industries*
- API, *Security Guidelines for the Petroleum Industry*, (2005)
- API, *Standard for Third Party Network Connectivity*, (2007)
- API Standard 1164*, Pipeline SCADA Security*, (2009)
- Center for Internet Security *Critical Security Controls (formerly SANS Top 20 Critical Security Controls)*
- Department of Energy (DOE) ONG Cybersecurity Capability Maturity Model (ONG C2M2)
- DOE *Energy Sector Cybersecurity Framework Implementation Guidance*, (2015)
- DOE Office of Cyber Security, Computer Incident Advisory Capability
- DOE, *21 Steps to Improve Cyber Security of SCADA Networks*
- *DOE Cybersecurity Procurement Language for Energy Delivery Systems*, (2014)
- DHS Control Systems Security Program, *Cyber Security Evaluation Tool* (CSET)
- DHS Chemical Facility Antiterrorism Standards, (2007)
- DHS, *National Infrastructure Protection Plan,* (2013)
- DHS, National Cyber Security Division (NCSD), *Catalog of Control Systems Security: Recommendations for Standards Developers,* (2010)
- DHS NCSD, *Cyber Security Procurement Language for Control Systems Security*, (2009)
- DHS Transportation Security Administration (TSA), *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, (2016)
- *DHS Cybersecurity Questions for CEOs*
- DHS Industrial Control Systems Cyber Emergency Response Team Recommended Practices
- International Organization for Standardization (ISO) and International Electrochemical Commission (IEC), *17799/27001/27002, Information technology - Security techniques - Code of Practice for Information Security Management*
- INGAA, *Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry*, (2011)
- National Association of Regulatory Commissioners Primer, *Cybersecurity for State Regulators* (2017)
- National Institute of Standards and Technology (NIST) SP 800 series
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-82, *Guide to Industrial Control Systems*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity*, (2014)
- North American Electric Reliability Corporation (NERC), NERC-CIP Standards
- TSA *Pipeline Security Guidelines*, (2011)