Testimony of
Kathy Judge
Director, Risk and Compliance, Corporate Security
National Grid

On Behalf of the American Gas Association

Before the
U.S. House of Representatives
Committee on Homeland Security
114th Congress

Pipelines: Securing the Veins of the American Economy

April 19, 2016

My name is Kathleen S. Judge and I am the Director, Risk & Compliance, Corporate Security for National Grid. National Grid is an international electricity and gas company based in the United Kingdom and northeastern United States that connects nearly 7 million customers to vital energy sources through its networks in New York, Massachusetts and Rhode Island. It is the largest distributor of natural gas in the Northeast. National Grid also operates the systems that deliver gas and electricity across Great Britain.

I have over 27 years of experience in the utility industry, and since 2007, I have been in physical security. I have been actively involved with the industry trade association security committees during my time in security, including serving on the American Gas Association Security Committee leadership team since 2011. I currently Chair the Oil & Natural Gas Sector Coordinating Council (ONG SCC) and Pipeline Working Group, which also serves as the Pipeline Sector Coordinating Council. I am also actively involved in the Edison Electric Institute (EEI) Security Committee and serve on the Executive Steering Committee for the Long Island Sound Area Maritime Security Committee. In 2014 and 2015, I was an active member on the NERC CIP 14 – Physical Security Standards Drafting Team.

I am testifying today on behalf of the American Gas Association (AGA). AGA, 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 95 percent - nearly 69 million customers - receive their gas from AGA members. Natural gas pipelines, which transport approximately one-fourth of the energy consumed in the United States, are an essential part of the nation's infrastructure. Indeed, natural gas is delivered to customers through a safe, 2.5 million mile underground pipeline system. This includes 2.2 million miles of local utility distribution pipelines and 300,000 miles of transmission pipelines that stretch across the country, providing service to more than 177 million Americans.

Natural Gas Utilities

Who We Are

Providing safe, reliable, and cost effective delivery of natural gas is the top priority of natural gas utilities across America. Given our strong service record, enviable safety statistics, and inherently resilient makeup due to the subsurface locations of the majority of our assets, natural gas utilities work vigilantly to maintain both the cybersecurity and physical security of the infrastructure. The natural gas system is a complex, interconnected, and well protected network of pipelines and associated facilities, including but not limited to, compressor stations, pressure regulators, pressure relief valves, and underground natural gas storage. Natural gas operations have a proven history of weathering natural events, accidental third-party damage, and intentional malicious assaults. Crisis management and site-specific security plans ensure operations are reinforced with well-trained workforce and system redundancies. Natural gas security professionals layer security measures within a framework of risk management. Further, natural gas owner/operators partner with Federal, state, and local government and law enforcement agencies to ensure effective and efficient response to events impacting natural gas operations.

The Transportation Security Administration (TSA) annual threat assessments have indicated that the threat against U.S. natural gas pipelines is low, and there is no current credible threat information regarding attacks on U.S. distribution pipelines. Further, the U.S. Department of Transportation (DOT) Bureau of Transportation Statistics continue to show pipelines as the safest form of transportation with very low incident rates, and the DOT Pipeline and Hazardous Materials Safety Administration (PHMSA), which regulates pipelines under its Office of Pipeline Safety (OPS), states that pipelines are one of the safest and most cost-effective means to transport the extraordinary volumes of natural gas. As such, pipeline safety and physical infrastructure security remain AGA's top priority.

Pipeline Risks

The primary objective for gas utilities is the safe and reliable delivery of natural gas to the consumer. As a result, natural gas utilities evaluate their security risks with public safety and natural gas interdependencies in mind. Pipeline security risks may be categorized as physical security risks or cybersecurity risks. In general, the leading security risks to natural gas utilities include, gas theft; access control; supply chain integrity; customer information theft; insider threat; facility and employee protection; and breach of Supervisory Control And Data Acquisition systems (SCADA), control systems, or communication systems. In addition, the potential for loss of telecommunications capability motivates the natural gas industry to maintain a basic level of manual operations, which adds a layer of security not afforded sectors that are fully automated.

Ironically, the leading risk to natural gas utility pipelines continues to be third party excavation damage. Excavation damage causes more casualties and service interruptions than any combination of security incidents.

While specifics may vary across companies, natural gas security professionals layer security measures in a handful of operational phases, i.e., planning, preparation, protection, incident response, and recovery that are framed by the overarching goal of risk management. The following provides more details about the activities associated with these phases.

- **Planning:**
  Natural gas owner/operators develop written programs that include methods for vulnerability and risk assessment, protection of sensitive information, threat responses, cooperation with public safety personnel, and physical security and cybersecurity practices.

- **Preparation Activities:**
  Natural gas owner/operators practice and prepare for extraordinary scenarios through participation in their own drills as well as those coordinated by industry, regional associations, and government agencies. Tabletop exercises enhance preparedness efforts and incident classification, while testing and engaging operators in restoration and recovery discussions. Finally, the industry participates in the TSA I-STEP[1] full-scale training and exercises designed to provide a forum for personnel to practice specific plans and procedures in response to security issues impacting their companies.

- **Protection Strategies:**
  Natural gas owner/operators make significant investments to protect their most critical assets. These investments focus on improving protection, detection, and perimeter security at the most critical locations. Examples of enhanced physical and personnel security measures include:
  - physical security measures such as, but not limited to and as appropriate, barriers and buffer zones, access controls, gates, locks and key controls, facility lighting, vehicle searches (static guards), surveillance cameras, intrusion detection and monitoring.
  - personnel security measures such as, but not limited to and as appropriate, biometric identification and badging, background investigation, training, exercises and drills.

[1] I-STEP: The Intermodal Security Training & Exercise Program is a “risk-based, intelligence-driven exercise, training and security planning solution in collaboration with other security partners to reduce risks to critical transportation infrastructure, and build and sustain security preparedness.”

- **Incident Response and Recovery:** Gas utilities have long maintained and been acknowledged for their consistent commitment to the safety of the natural gas infrastructure, workers and processes. The commitment to operational resiliency is equally substantial. Redundancies along the delivery system provide operators the flexibility to reduce pressure and redirect, shut down, or restore gas flow. Facilities for alternative fuels and natural gas storage provide additional options to supplement gas supply to minimize service disruption. Companies also have critical back-up and replacement equipment and parts stored at key points along a system. Rapid response teams can be quickly deployed to get the system up and running in order to reduce downtime. Overall, the industry approaches preparedness and response from the local level, acknowledging that events impact workers, businesses and communities first and foremost. While resources and information are often held at the regional or national levels, it is the local facility operators who have the best ability to assess their systems, identify needs, and execute the work needed to restore services.

  Title 49 of the Code of Federal Regulations governs the response aspect of security planning. Pipeline companies have years of experience responding to emergency incidents and are required by DOT to have effective emergency plans in place. Operators are also required to report significant incidents - those resulting in serious injury, loss of life, or property damage greater than $50,000 - to the DOT National Response Center (NRC). A mechanical failure or unintentional act resulting in significant damage to a pipeline will be reported to DOT through the NRC. An intentional act of damage, or act of a suspicious nature involving a pipeline, will be reported to TSA through the Transportation Security Operating Center (TSOC).

  Responding to a pipeline failure caused by an intentional act varies little from the response to a mechanical failure or an unintentional act; except that, operators must exercise caution recognizing the incident may be criminal in nature. Facility restoration is the final component of an industry security initiative. Specific plans will vary among operators based on the criticality of the pipelines and factors such as location and time of year.

Security is woven into corporate governance through security policies, incident procedures, recordkeeping, communication, security measures embedded within design and construction practices, as well as equipment maintenance and testing. To help maintain operational security, natural gas utilities are careful not to publicize clearly sensitive information about critical infrastructure that might provoke new threats, or endanger the safety of the American public or the integrity of the nation’s gas systems. Gas companies work closely with law enforcement personnel and first responders on site-specific security plans and security drills. Additionally, gas utilities participate in security information sharing communities such as the Downstream Natural Gas Information Sharing & Analysis Center, which provides participants with timely situational awareness, intelligence analytics, and industry incident information exchange.

Sector Coordinating Council

In 2004, Sector Coordinating Councils were formed to coordinate security initiatives among the Nation's critical infrastructure assets. The Oil and Natural Gas Sector Coordinating Council (ONG SCC) was formed by 19 industry trade associations to provide a forum for discussion and to coordinate communications between industry security professionals and representatives of the Energy Sector Government Coordinating Council (Energy GCC[2]). Subsequent to the formation of the ONG SCC, the Pipeline Working Group (Pipeline Sector Coordinating Council) was formed to further enhance communication and collaboration among pipeline operators and government entities.

Cooperation

The pipeline industry takes its responsibility for facility, system, and network security very seriously. The TSA provides guidance and expectations for the practices and procedures necessary to secure the Nation's critical pipeline infrastructure. Members of industry and trade associations, working together and through the SCCs, have developed guidelines that are consistent with these expectations. The typical operator has a developed security program, has conducted facility risk assessments, and has implemented sound practices that provide for effective and practical system security.

The natural gas industry supports a process for raising public awareness about pipelines in a manner that does not jeopardize security, interstate commerce, or proprietary business information. In addition to close coordination amongst gas utilities to reinforce operational resilience, the industry works directly with government partners in DHS, DOE, the White House, the government intelligence community, and local and state law enforcement agencies to more thoroughly understand potential threats and to better protect its systems. AGA and gas industry representatives actively participate in interdependency initiatives coordinated by Federal and state governments to enhance preparedness, response, and recovery planning. For example, in 2010 and in support of the objectives of the National Infrastructure Protection Plan, owner/operators across the oil and natural gas sector collaborated with DHS and DOE to present several cross-sector emergency management workshops aimed at promoting an integrated private sector and government response during natural disasters and terrorist incidents. The gas industry also engaged with DOE, DHS, electric utility operators, and local law enforcement on a series of physical security and cybersecurity briefings across the United States and Canada. These briefings allow government officials to provide information on the current threat environment, discuss mitigation strategies, and encourage participants to further develop relationships with first responders and industry partners. Additionally, many utility security personnel hold government security clearances, which allow access to classified threat information to further develop security strategies.

[2] Energy GCC: The Energy Sector Government Coordinating Council is chaired by a representative of the Department of Energy, and the GCC includes members of numerous agencies, including TSA and DOT.

Resilience

Resilience is an integral element of the gas industry's critical infrastructure protection mission that is bolstered by multiple layers of safety and reliability mechanisms to reduce the magnitude and/or duration of disruptive events and to ensure sufficient backup coverage exists. Because utilities must "expect the unexpected," they have all-encompassing contingency plans for dealing with man-made and natural disasters to help ensure natural gas will flow safely and reliably. The industry continues to work with federal agencies to enhance the physical security and cybersecurity of its critical infrastructure while remaining firmly committed to taking appropriate and measured actions to deter threats, mitigate vulnerabilities, and minimize consequences associated with a terrorist attack and other disasters.

The National Infrastructure Advisory Council's *Critical Infrastructure Resilience Study* found that the oil and natural gas sector has a significant amount of redundancy and robustness built into the system. Most pipelines are relatively easy to repair over the short-term and in many cases, alternative routes are also available to move sufficient amounts of product around the site of an incident, thus preventing major disruptions. Moreover, redundancies are built into the pipeline infrastructure, including interconnects between companies. This planning and interconnect capability ensures consumers with reliable service.

Transportation Security Administration

Pipeline Security Authority

Under the provisions of the Aviation and Transportation Security Act (Public Law 107-71), TSA was established on November 19, 2001, with responsibility for civil aviation security and "security responsibilities over other modes of transportation that are exercised by the Department of Transportation." To fulfill this mandate in the pipeline mode, on September 8, 2002, TSA formed the Pipeline Security Division, which is now called the Pipeline Section of the Office of Security Policy and Industry Engagement (TSA Pipeline Section).

Partnership

The vast majority of critical infrastructure is privately owned and operated. As such, effective public-private partnerships are the foundation for critical infrastructure protection and resilience strategies comprising timely, trusted, unguarded information sharing among stakeholders. The TSA Pipeline Section recognized early on that the pipeline industry security professionals are charged with a parallel objective, i.e., protect the critical infrastructure, and this is best accomplished in a collaborative environment. Historically, TSA has strategically refrained from executing its regulatory authority and, instead, pioneered a path of genuine government partnership with pipeline owners/operators. Fourteen years later, this approach continues to serve as a model for public/private partnership that offers collaboration, mutual support, and measurable achievement towards a common goal – pipeline security.

The partnership approach has established a bond between industry and government that is uncommon across the government/operator community and is measurably beneficial for all stakeholders. The operator knows best his/her operations – what needs to be secured and how to best achieve this; TSA provides valuable tools, knowledge resources, insights, and perspectives that advances the operator's decision-making process. The end result is an improved security posture that benefits all involved, except the adversary.

Programs/Tools/Products

TSA has many programs, tools, and products available to assist pipeline operators in addressing security matters. The portfolio includes, Critical Facility Inspections (CFI), Corporate Security Reviews (CSR), Critical Facility Security Reviews (CFSR), Blast Mitigation, Smart Practices, I- STEP, monthly stakeholder teleconferences, Security Awareness Training Videos, and the International Pipeline Security Forum. These resources bring government and operators together and foster relationships and cooperative efforts that have been key to advancing industry pipeline security practices.

TSA Pipeline Security Guidelines

The leading tool in the TSA portfolio is the *TSA Pipeline Security Guidelines* (*Guidelines*), a product of collaboration that coalesced the institutional knowledge and experience of pipeline security professionals with the resources of the federal government. The *Guidelines* were developed with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties and represent TSA's expectations of industry. TSA released the *Guidelines* in December 2010 (re-released in April 2011), and it applies to natural gas distribution pipelines and liquefied natural gas facilities. Notably, the partnership between pipelines and TSA effectively drives industry to advance beyond minimum security standards to the deployment of smart industry practices. The *Guidelines* provides operators the flexibility to secure pipeline infrastructure by applying practices that are most applicable to their individual systems.

Onsite Reviews/Visits

Equally significant in advancing industry's security posture are non-regulatory, onsite facility reviews/visits. The CSRs and CFIs have historically been the program names for these reviews/visits conducted by the TSA Pipeline Section. The CSRs focused on the operators' overall security plan. The CFIs focused on security plan implementation and actual day-to-day security practices at critical facilities. More recently, CFIs have been renamed as CFSRs.

The CSRs are designed for TSA to focus on an operator's overall security plan implementation through: 1) learning more about an organization's pipeline system, 2) reviewing an organization's listing of critical facilities, 3) discussing at length the details of an organization's security plan and programs and 4) engaging with the operator to familiarize the operator with TSA and vice-versa prior to any security-related event or emergency. Following the review, TSA shares observations with that company, including a security benchmark so the company can compare itself with similar or peer companies. TSA discusses areas in which they observe the company excelling in relation to the industry and smart practices. TSA also identifies areas in which the company is observed to be lacking and will make recommendations based on the *Guidelines* or offer considerations based on their expertise and industry observations. TSA then follows up with each organization to see what progress has been made based on their recommendations.

CFSRs are site by site walkthroughs at each critical facility focused on site specific security plans and measures. Following each review, TSA sends a report to the operator including commendations and recommendations. TSA then follows up with each operator to check in on the progress of recommendations. TSA also utilizes information obtained during the reviews to develop security smart practices that are shared with the industry.

The review/visits offer TSA a unique opportunity to engage in open, candid, non-punitive discussions with the operator. This affords TSA with a more holistic view of how the industry can be effective in its flexible use of the *Guidelines* and reinforces the fact that constructive exchange between TSA and the operator is more useful for security planning than the ‘us versus them’ compliance-audit environment. Results of these reviews have been used to develop security "smart practices" that are shared widely throughout the industry. These programs have not only been a means of evaluating the actual security practices of the pipeline operators but have also been a means of promoting industry familiarity with the responsibilities and personnel of TSA. Thus, the collaboration between TSA and the pipeline operator is a mutually beneficial relationship that cannot be undervalued.

Stakeholder Teleconferences

For wider participation, TSA holds monthly stakeholder calls to share physical and cyber threat and intelligence information with industry. Following notable security events, TSA conducts more frequent calls and sends out relevant information to industry stakeholders.

Additional Engagement Opportunities

Industry and TSA annually convene to go through the Transportation Sector Security Risk Assessment. This exercise includes evaluating a list of scenarios and determining the likelihood of such an event. Both also collaborate on the development of Pipeline Modal Threat Assessment prepared by the TSA Office of Intelligence and Analysis.

In addition to the *Guidelines* and TSA products, the pipeline industry references and implements multiple resources, programs, and standards from wellhead to the meter as appropriate for the company’s operations. Such resources include American Petroleum Institute Recommended Practices and standards, DOE Oil & Natural Gas Cybersecurity Capability Maturity Model, SANS Institute cybersecurity standards, and the North American Electric Reliability Corporation Critical Infrastructure Protection Committee standards. The pipeline industry also coordinates initiatives with other critical infrastructure sectors, including but not limited to Chemical, Energy, Communications, and Financial Sectors as well as other modes within the Transportation Sector.

To Regulate or Not To Regulate

The formula that promotes ongoing improvements to the pipeline industry's security posture consists of the partnership, the *Guidelines*, and the operator facility visits by TSA.

> The *Guidelines* has a common goal with the pipeline operator to promote the security pipeline infrastructure while recognizing operational, structural, and commodity differences across the pipeline industry. This performance-based approach supports the flexibility needed for operators to address the dynamic security threats specific to their operations in different operating settings.
>
> The CSRs, CFIs and CFSRs demonstrate the owner/operators' actions to follow the *Guidelines*. According to TSA, there have been 347 CFIs, 154 CSRs, and 151 CFSRs to date. Each of the visits resulted in TSA recommendations to the operator to which 85-90% of the recommendations have already been addressed by the operator, and the remaining recommendations are in the process of being addressed, or the operator found a better way of achieving the objective of the recommendation. TSA has gone on record stating that based on its CSRs and other information, pipeline operators already employ most of these recommendations in their security plans and programs.

In addition to partnering with TSA, pipelines must comply with DOT pipeline safety regulations, which require the incorporation of system fail-safes that in many cases protect against the goals of the adversary; in the case of natural gas utilities, this would apply to system over-pressurization. Intrastate pipeline must also comply with state pipeline safety regulations that go above and beyond DOT's regulations.

Improving on TSA's Role

In January 2014, TSA announced a significant organizational realignment that dismantled effective programs (previously highlighted) and processes both the government and the operators had benefited from. During the realignment, it was the intent of DHS to have generalists (i.e., TSA representatives who work all transportation modes) to conduct the CFSRs. In practice, this proved ineffective as the visits focused more on educating the TSA generalist about pipeline security than on bilateral value gained. Ostensibly, the impetus for the realignment was to sustain TSA's effectiveness and to remove the stove-piping amongst the various modes. Industry representatives expressed concern over the reorganization, as this realignment was done without engagement of the operator community.

AGA worked with Congressional staff and TSA staff to facilitate a meeting between TSA leadership and industry to discuss the reorganization. After extensive pressure from pipeline operators and a measurable decline in TSA's engagement with industry, TSA reversed the realignment and returned to a model similar to the original. Because most of the original well-trained TSA pipeline staff had been reassigned elsewhere, the program is slowly rebuilding. AGA credits the leadership of Ms. Sonya Proctor, Director, Surface Division, Office of Security Policy and Industry Engagement, for recognizing the ineffectiveness of the realignment, the need to return to the original model, and the need to fill open pipeline security positions with qualified candidates. TSA is strongly encouraged to ramp up the CFSR program with reviewers who already understand pipeline operations, as was the case prior to the realignment efforts.

Further, industry has invested a great deal of resources working with the government intelligence community to ensure the timely sharing of actionable information. Though certain groups, such as DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), recognize the value of this, others within the intelligence community (outside of DHS) do not necessarily agree. TSA should be positioned and empowered to be a conduit of threat information that has implications to pipeline operations. This would include information that could impact sectors/infrastructure upon which pipeline operations are dependent or which have operations similar to pipelines, e.g., SCADA. Along these same lines, more government resources should be invested to provide well-trained and equipped pipeline security professionals across the Nation to conduct more facility reviews and noncompliance visits.

PHMSA

Security and safety go hand-in-hand. As prescribed in Title 49 of the Code of Federal Regulations, pipeline safety, including emergency management, has been the purview of DOT through PHMSA's Office of Pipeline Safety. Prior to events of September 11, 2001, the Homeland Security Act of 2002, Homeland Security Presidential Directive 7 (December 17, 2003), and the Aviation & Transportation Security Act of 2001, pipeline security was under the purview of DOT, where it played a less prominent role than pipeline safety. In September of 2004, a Memorandum of Understanding (MOU) was signed by representatives of DHS and DOT memorializing an agreement of respective pipeline security roles and responsibilities; "DOT and DHS will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)." Additionally, in August 2006, an MOU was signed by TSA and PHMSA to clarify that TSA has primary responsibility for pipeline security and formalize coordination between TSA and PHMSA to ensure that pipeline security and pipeline safety complement one another: "PHMSA is responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation including identifying pipeline safety concerns and developing uniform safety standards."

The emergency response practices prescribed by DOT are used in the event of any incident, whether intentional or accidental. All involved parties must work cooperatively with law enforcement, local agencies, and first responders to minimize damage and danger to local communities and critical facilities.

Coordination

For a number of years following the 2006 MOU, PHMSA was actively engaged with TSA activities, including the development of the *Guidelines*. However, more recent experiences suggest that PHMSA has lost its focus on cybersecurity. For example, PHMSA has proposed significant changes to its National Pipeline Mapping System that would require operators to provide very detailed pipeline operations and location information, including information on critical valves, online in a single database, and this information would be made widely available. PHMSA's actions suggest pipeline cybersecurity is an afterthought rather than part of the evaluation process.

Summary

Natural gas utilities value the collaborative security relationship they have with TSA. TSA is to be commended for choosing the more constructive path, i.e., partnering with owners/operators, to improving the pipeline sector's security posture. Furthermore, compliance does not equate to security. The formula for the measurable effectiveness of TSA is the result of practical guidelines, smart practices, information exchange, and trusted engagement with the private sector. TSA should continue the process of reversing its earlier realignment efforts and return to the model of a dedicated group of TSA staff with knowledge and experience in pipeline operations specifically assigned to pipeline security. TSA should also continue to coordinate with PHMSA where pipeline security and pipeline safety overlap. Along the same lines, PHMSA should be more proactive in consulting with TSA on pipeline safety matters, in particular regarding regulations that have security implications and may increase pipeline vulnerability.