

**Federal Energy Regulatory Commission
Security Investments for Infrastructure Technical Conference
March 28, 2019**

Panel I: Cyber and Physical Security, Best Practices, and Industry and Government Engagement

**Donald Santa
President and CEO**

Interstate Natural Gas Association of America

Good morning, the Interstate Natural Gas Association of America (INGAA) appreciates the opportunity to address the Commission and senior officials of the Department of Energy on the important topic of current cyber and physical security practices to protect energy infrastructure. My comments on behalf of INGAA will focus on the protection of interstate natural gas pipelines.

The Role and Importance of Natural Gas

Natural gas is one of the pillars of our nation's economy and natural gas transmission pipelines are the indispensable link between the suppliers and consumers of this essential energy resource. Pipelines are the only cost-effective means to transport natural gas long distances over land.

The diversity of natural gas' end use makes it unique among the nation's energy resources -- natural gas supplies 76 percent of residential and commercial energy consumption; 45 percent of industrial energy consumption; and 35 percent of the electricity generated in the United States. The operators of interstate natural gas pipelines appreciate the significant and growing utilization of natural gas to generate electricity and the resulting effect on the criticality of their infrastructure to the nation's security.

Security is a Priority for the Natural Gas Pipeline Industry

Pipeline operators carefully evaluate and take steps to mitigate risks that threaten their systems. This is true across the board, whether it be risks to the safety and integrity of the pipeline, risks caused by extreme weather, or risks caused by physical and cyber security threats.

The boards of directors and senior management of INGAA's member companies have identified cybersecurity as a top enterprise risk. It is widely recognized that the potential cost of recovering from a security incident far exceeds the cost of implementing measures to mitigate those risks.

Because a trade association can be the focal point for collective industry action, pipeline security has become a priority for INGAA as well. Last year, INGAA's Board of Directors adopted the Commitments to Pipeline Security, a statement that enumerates the actions that all member companies are taking as part of their security programs. This statement emphasizes member companies' commitments to:

1. following the Transportation Security Administration's (TSA's) Pipeline Security Guidelines;
2. following the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework; and
3. engaging in information sharing across the industry and with our federal partners.

This final commitment is important. Strong coordination and cooperation in support of information sharing across the private sector and the federal government is foundational to understanding how best to protect our infrastructure.

Evolving Threat Landscape

Risk prioritization starts with an understanding of the threats. Once we better understand the threats, we can determine how to implement the security controls that will enable us best to deter, delay, respond to and recover from the incidents that could result from those threats.

Threats are evolving. Not very long ago, the biggest threats to pipeline operators were the threat of physical damage from a third-party excavator and the threat of financial data compromise from cyber criminals.

We now are concerned with the threat from sophisticated, well-resourced nation state actors. These threat actors are motivated and have the technical means to develop zero-day malware that can go undetected in a system for long periods as well as the means to launch coordinated physical attacks on our systems.

We also have seen an increase of domestic threats to our infrastructure from groups that wish to make political statements by damaging our infrastructure and delaying our projects. They too employ a variety of evolving techniques, such as flying unmanned aircraft systems into restricted areas, using manipulative online tactics to acquire confidential data, and streaming acts of vandalism on social media.

In both cases, the ongoing dialogue with our federal partners is an essential part of an effective response. Pipeline operators rely on our federal partners to share important information about the tactics and techniques used by our adversaries as well as the mitigative measures needed to reduce the risk of a successful attack by these threat actors.

The emergence of well-resourced, determined nation state actors as a principal security threat to the nation's energy system and our national security place a premium on collaboration and cooperation with our federal partners. This threat is beyond that which the private sector can be expected to confront on its own and goes to the very heart of the role of the federal government in protecting the security of our nation.

Potential Consequences Must be Considered

In addition to understanding the threats, it is important to understand the potential consequences should an attack be successful. In this context, that means understanding how pipelines are designed and operated.

Experience tells us that the incidents affecting pipeline transportation have an isolated impact on the natural gas system. While customers in the immediate vicinity of an incident may be affected, the natural gas system has never experienced anything approaching the scope and consequences of an electric blackout.

The physics of the natural gas system are completely different than the physics of the bulk electric system. This lends itself to fundamental differences in how the systems are balanced. While the electric system must be balanced in a matter of seconds, the natural gas system has hours or more, allowing time to isolate an impacted pipeline and re-direct gas around the affected area or from other supply sources.

In addition, pipeline operators have the means to limit the effects of an incident, including the ability to isolate sections of a pipeline, the frequent availability of multiple pipeline pathways to re-route gas, and the diversity of sources of supply and underground natural gas storage, to name a few. Furthermore, the same design elements and processes mandated for natural gas pipelines to protect public safety also would mitigate the impacts of a security intrusion.

Therefore, even if one assumes that a malicious threat actor compromises a pipeline company's cyber defenses and succeeds in accessing its SCADA system, the combination of the layers of protection designed into a pipeline to prevent a catastrophic failure, the physics of natural gas, and the ability to operate the system locally (without SCADA) greatly mitigate the threat that the gas system could be disabled by a cyberattack.

None of this is to say that natural gas pipeline operators take the threat of physical and cyberattacks lightly. The point only is that risk cannot be fully understood without an appreciation of the potential consequences, which are very different for the natural gas system compared to the bulk electric system.

Recovery of Pipeline Operator Costs for Physical and Cyber Security

From a legal perspective, the recovery in an interstate natural gas pipeline's maximum lawful rates of costs prudently incurred to protect the physical and cyber security of the pipeline is no different from the recovery of other costs that are part of the pipeline's cost of service.

A practical impediment to recovery, however, can be whether a pipeline's maximum lawful rate will clear the market; many pipelines must discount their rates to meet competition from other interstate and, in some cases, intrastate pipelines. In other cases, pipelines have negotiated rates; whether such a rate can be increased to reflect additional costs is governed by the terms of a pipeline's contracts with its shippers. Most negotiated rate contracts do not allow for adjustments in either direction to reflect changes in costs. This contrasts with rates for electric transmission, and especially transmission within ISOs and RTOs, which rates are established on a region-wide basis and in which costs are socialized among all ratepayers.

The Commission's 2001 Policy Statement on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies provides the flexibility necessary for pipelines to address unique circumstances in seeking to recover such costs. Affirmation of the continued applicability of the 2001 policy statement would be welcome.

Conclusion

The natural gas pipeline operators represented by INGAA recognize that the natural gas system is critical to our nation's economy, to the health and welfare of its citizens and to our national security. These pipeline operators are committed to ensuring the security, reliability and resilience of this infrastructure. As part of that, these pipeline operators are committed to coordinating with our electric industry

counterparts as we plan for how to protect this infrastructure from rapidly evolving threats. An essential element of this preparedness is sharing threat information across our industry, across economic sectors and in a robust two-way dialogue with our federal partners.

As part of that, these pipeline operators are committed to coordinating with our electric industry counterparts as we plan for how to protect this infrastructure from rapidly evolving threats. An essential element of this preparedness is sharing threat information across our industry, across economic sectors and in a robust two-way dialogue with our federal partners.