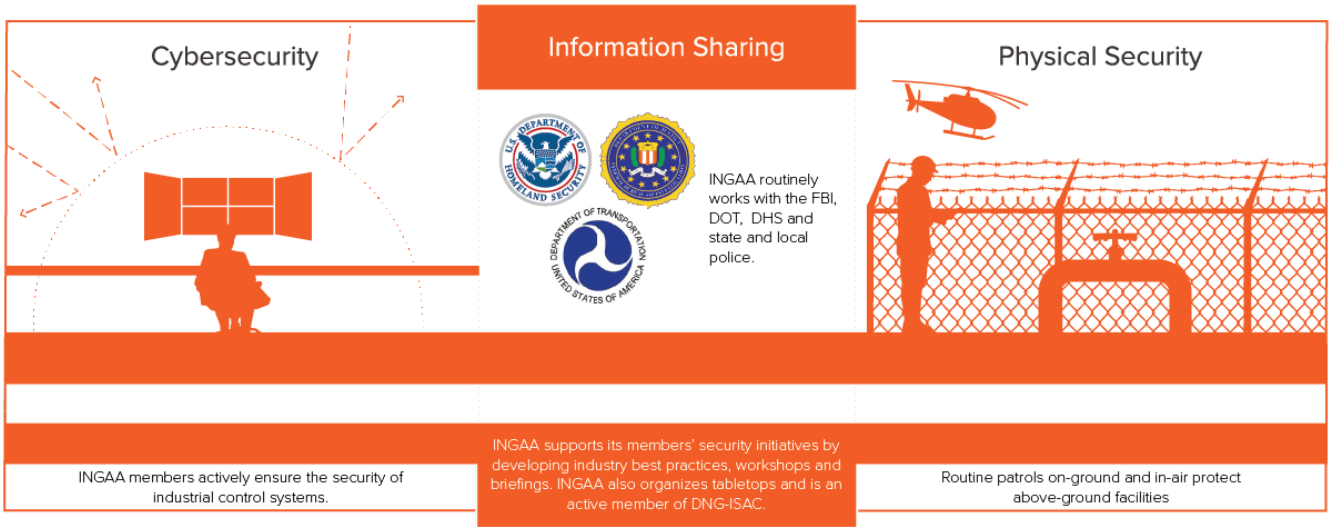
Pipeline Cyber & Physical Security

Interstate Natural Gas Association of America

INGAA and its member companies work diligently to secure and protect their cyber and physical assets. Whether the threat stems from a natural event, terrorist activity or a cyber attack, the design and operational attributes of the natural gas pipeline system reduce the likelihood of an adverse effect on a locality or the nation.

INGAA and its members are strongly committed to ensuring the security, reliability and resilience of natural gas transmission pipelines.



Guarding America's Pipelines Against Cyber Threats

The pipeline industry takes the security of our systems very seriously. INGAA and its members work collaboratively and regularly with government agencies to share information about threats and best practices for protecting and enhancing critical energy infrastructure.

The Transportation Security Administration (TSA) – in collaboration with the Department of Homeland Security and the Department of Energy – has established a cross-agency partnership to conduct comprehensive pipeline cybersecurity assessments through the Pipeline Cybersecurity Assessment Initiative. This initiative provides a valuable tool for industry and government to identify trends and assess the unique cybersecurity risks that pipeline operators face. Through the collective expertise of these three agencies, INGAA believes this initiative will lead to a better understanding of risks, better-informed actions to address them and added opportunities to strengthen our security posture as an industry. We believe that a risk-informed approach is the best and most effective way to protect our systems and assets against rapidly evolving cyber threats. INGAA and its members support this program by volunteering for assessments and agreeing to partner continuously with government agencies on identifying how to improve our security posture.

Pipeline Cybersecurity Assessment Initiative

Transportation Security Administration

Strong collaboration between industry and government is key to ensuring successful mitigation of cyber risks. Government agencies have wide access to classified threat intelligence and a broad understanding of practices and approaches for mitigating cybersecurity risks across all critical infrastructure. Industry owns and operates critical infrastructure and best understands the uniqueness of its assets as well as what is practical and implementable to protect its infrastructure.

In March of 2018, TSA released an update to its Pipeline Security Guidelines to address the latest practices and understanding of cybersecurity threats. Strong collaboration between industry and government helped facilitate this timely, meaningful and practical update to the guidelines.

> ***"In this environment of rapidly evolving cyber threats, it is important that we take an approach that enables flexibility and allows us to quickly adapt and update protocols ... We need the flexibility and ability to build on our baseline practices to look forward towards addressing the threats of the future."***
>
> ***-Don Santa***

INGAA member companies diligently deploy a multifaceted security strategy to secure and protect critical energy infrastructure:

- Pipeline operators implement the National Institute of Standards and Technology, or NIST, cybersecurity framework to optimize security and resilience of critical infrastructure. Published in 2014, the NIST framework offers a standardized security approach for all critical infrastructure in the United States, outlining ways to employ five strategic functions: identify, protect, detect, respond and recover.
- Pipeline operators share information across the industry in real-time, ensuring rapid response to security incidents and threats. Operators use resources like the Downstream Natural Gas Information Sharing and Analysis Center and the Oil and Natural Gas Information Sharing and Analysis Center to share threat intelligence and recommended mitigations.
- Pipelines have plans in place to ensure systems can continue to operate in the event of an outage of a Supervisory Control and Data Acquisition (SCADA) system. This means that even when these computer systems are unavailable, operators can keep gas flowing.
- Pipeline operators maintain backup control rooms and backup data rooms at alternate locations to ensure quick recovery in the event of a successful cyber intrusion.
- Operators take advantage of a number of assessment opportunities, through the TSA and the Federal Energy Regulatory Commission, as well as other peer reviews and third-party assessments in order to identify opportunities to improve their security programs.

Ensuring Reliable Delivery of Natural Gas

Pipeline transportation service is extremely reliable:

- The underground interstate pipeline network is protected from extreme weather events and is linked to various supply sources, offering avenues to keep gas flowing in the rare event of an outage.
- INGAA members use fences, routine foot and aerial patrols and continuous monitoring to protect above-ground facilities like compressor and meter stations and rights of way.

Learn more about physical pipeline safety efforts by reading our Pipeline Safety and Reliability fact sheet.

Did you Know?

Between 2006 and 2016, pipelines delivered **99.79%** of "firm" contractual commitments to primary delivery points, according to a 2017 Natural Gas Council report.