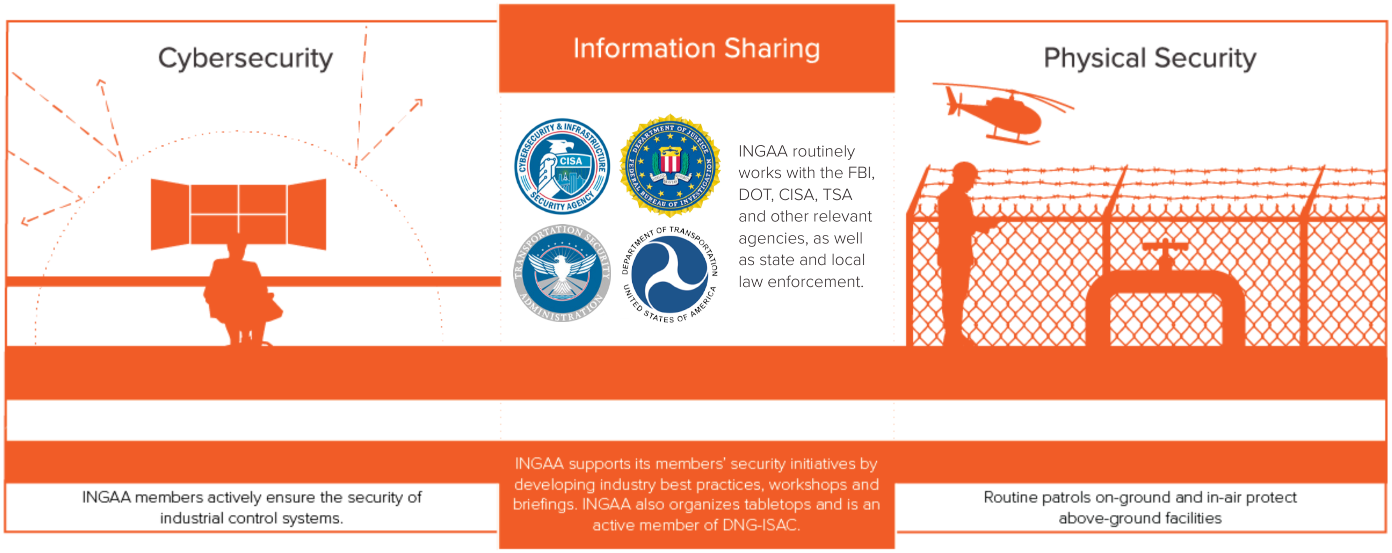
Pipeline Cyber & Physical Security

INGAA
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, criminal or 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.



Cybersecurity

INGAA members actively ensure the security of industrial control systems.

Information Sharing

INGAA routinely works with the FBI, DOT, CISA, TSA and other relevant agencies, as well as state and local law enforcement.

INGAA supports its members' security initiatives by developing industry best practices, workshops and briefings. INGAA also organizes tabletops and is an active member of DNG-ISAC.

Physical Security

Routine patrols on-ground and in-air protect above-ground facilities

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 Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) and the Department of Energy (DOE) – has established a cross-agency partnership to conduct comprehensive pipeline cybersecurity assessments, called Validated Architecture Design Reviews (VADRs), through the Pipeline Cybersecurity Initiative (PCI). VADRs are 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 supports a better understanding of risks, 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 participating in assessments and agreeing to partner continuously with government agencies on identifying how to improve our security posture.

CISA also works with pipeline companies through the voluntary CyberSentry program, which was developed to enhance the cyber resilience of organizations that own or operate critical infrastructure. CyberSentry uses sensors to continuously monitor the Information Technology (IT) and Operational Technology (OT) networks of a participating partner for cybersecurity threats.

> *"Through focused investment in the security of our nation's natural gas delivery system, we can continue to strengthen and protect this critical energy infrastructure. Modern regulatory policies should facilitate ongoing investment and provide operators the flexibility needed to nimbly respond to and address today's rapidly evolving cyber threats."*
>
> *- Amy Andryszak, President and CEO*

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. Bi-directional threat information sharing between the government and private sector is a foundational component to facilitating this partnership. Given the private sector owns and operates approximately 85% of all critical infrastructure assets in the United States, owner/operators have the first-hand knowledge necessary to best protect these assets, including what is practical and implementable to protect their infrastructure.

In March of 2021, TSA released an update to its Pipeline Security Guidelines to address new criteria for identifying critical pipeline assets. This update builds on previous iterations of the Pipeline Security Guidelines to assist owner/operators in applying the latest practices and understanding of cybersecurity and physical security threats. Strong collaboration between industry and government helped facilitate this timely, meaningful and practical update to the guidelines.

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 (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. NIST also periodically releases and updates Special Publications (SPs) specific to OT and industrial control systems (ICS) operations, which are frequently used by INGAA members.
- 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 (DNG ISAC) and the Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC) 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 TSA, CISA, DOE, and the Federal Energy Regulatory Commission (FERC), as well as other peer reviews and independent third-party assessments in order to identify opportunities to improve their security programs.
- INGAA members participate in government-led cyber and physical security exercises, including GridEx, CyberStrike, and Clear Path, to help the industry respond cohesively to threats in a way that ensures energy security and resilience.