Commitments to Pipeline Security

Interstate Natural Gas Association of America

The Interstate Natural Gas Association of America (INGAA) and its members are committed to promoting the security, reliability and resilience of interstate natural gas transmission pipelines.

INGAA members implement security programs and take action to ensure pipeline infrastructure remains resilient and secure. INGAA members use security standards, guidelines and information-sharing resources, including: 1) the Transportation Security Administration's *2018 Pipeline Security Guidelines*; 2) National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*; and 3) information-sharing platforms, including the Downstream Natural Gas Information Sharing and Analysis Center and the INGAA Automated Threat Information Sharing Network Pilot Program. These actions help secure pipelines against cyber and physical security threats as well as natural disasters like hurricanes or floods.

INGAA's members commit to the following actions:

Identify

Develop the organizational understanding to manage security risk to systems, assets, data and capabilities.

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. Gather intelligence and share information

Protect

Develop and implement the appropriate safeguards designed to ensure delivery of critical infrastructure services.

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

Detect

Develop and implement appropriate activities designed to identify the occurrence of a security event.

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

Develop and implement appropriate activities to take action in a security event and restore critical services.

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