ONG
PHYSICAL SECURITY 101

Oil & Natural Gas owners and operators are committed to help ensure that critical infrastructure remains resilient to emerging physical security threats. Industry proactively collaborates with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving our security posture.

ONG owners and operators implement risk based security programs and actively engage in actions to help enhance the security of ONG infrastructure which spans all 50 states with diverse geographic and operating conditions. The Department of Homeland Security Transportation Security Administration (TSA) has oversight for security of pipelines, and as such, has developed the *TSA Pipeline Security Guidelines*. Industry implements these guidelines as applicable to their individual environments. Additionally, industry utilizes a number of available security standards, models, guidelines, and information sharing resources, including, but not limited to: TSA Pipeline Security Smart Practices Observations, TSA Intermodal Security Training Exercise Program (I-STEP), and Information Sharing and Analysis Centers (ISACs).

Below are voluntary security actions that are being taken by individual owners and operators to help ensure the secure operation of infrastructure. It is the consensus of industry that the actions and accompanying elements listed below enhance the resilience of a company's operations to security threats. However, the method and timing of implementation of these actions will vary with each operator. Each operator evaluates, and implements as appropriate, these actions taking into account individual environments, identified risks, and what has been deemed reasonable and prudent.

IDENTIFY

1. Establish ownership, sponsorship, organizational roles and responsibilities for corporate security programs
2. Conduct criticality assessments to identify and rank critical facilities
3. Define security roles, responsibilities, and lines of communication
4. Intelligence gathering and information sharing

PROTECT

Review security plans and procedures

1. Implement access controls
2. Implement personnel training and awareness programs
3. Develop & implement maintenance program
4. Incorporate security into system designs

DETECT

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

1. Develop communications plans for security events
2. Conduct periodic drills and exercises
3. Plan for restoration of facilities and assets
4. Establish redundancies for resilience
5. Establish procedures for responding to threat information and actual events

OIL AND NATURAL GAS SUBSECTOR COORDINATING COUNCIL