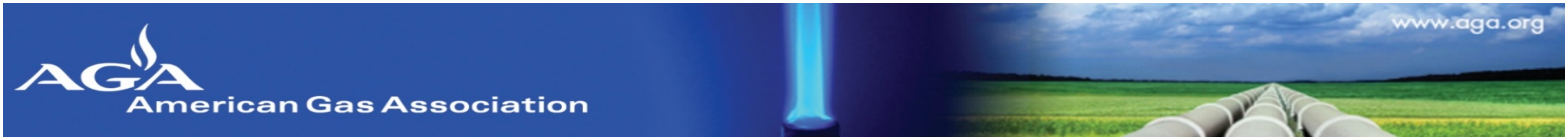

AGA's Commitment to Cyber and Physical Security

AGA and its members are dedicated to help ensure that natural gas pipeline infrastructure remains resilient to growing and dynamic cyber and physical security threats. We are committed to proactively collaborating with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving our security posture and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

AGA and its operators implement security programs and actively engage in voluntary actions to help enhance the security of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions. The Department of Homeland Security Transportation Security Administration (TSA) has oversight for security of pipelines (including natural gas distribution and transmission), and as such, has developed the *TSA Pipeline Security Guidelines*. AGA member gas utilities and transmission companies are implementing these guidelines as applicable to their individual environments. Additionally, AGA members are utilizing a number of available security standards, models, guidelines, and information sharing resources, including, but not limited to: (1) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, (2) Department of Energy Cybersecurity Capability Maturity Model (C2M2), (3) Department of Homeland Security Industrial Control System Computer Emergency Readiness Team (ICS-CERT), (4) TSA Pipeline Security Smart Practices Observations, and (5) TSA Intermodal Security Training Exercise Program (I-STEP). In addition, AGA gas utilities and transmission companies will be part of the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) by 2017.

Below are voluntary security actions that are being taken by AGA or individual operators to help ensure the secure operation of natural gas pipeline infrastructure. AGA and its operators recognize the significant role state regulators or governing bodies play in supporting and funding these actions. It is the consensus of AGA members that the actions and accompanying elements listed below enhance the resilience of a company's gas 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 by their state regulators or governing bodies.

IDENTIFY

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. Intelligence gathering and information sharing

PROTECT

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

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 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