ONG CYBERSECURITY 101

As owners and operators of critical energy infrastructure in the United States and globally, cybersecurity is a high priority for the oil and natural gas (ONG) subsector. All along the value chain, the ONG subsector actively employs a wide portfolio of security standards, models, guidelines, and information sharing resources to remain resilient to growing cybersecurity threats.

RISK MANAGEMENT

In general, owners and operators work to tailor their cyber risk management to their company's assets and potential risks, allowing for flexibility to respond to ever-changing threats. Cybersecurity is evaluated as a business risk and treated by the ONG subsector Boards of Directors and senior executives as a leading priority.

The subsector acknowledges that different segments of the ONG value chain carry different levels of risk, which require modified risk management strategies. Most companies within the ONG subsector belong to one or more trade associations that represent segments of the value chain.

The ONG subsector also builds its cyber risk management around cyber guidance developed by industry, security standards, models, guidelines, and program products that include, but are not limited to:

- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
- U.S. Department of Energy Cybersecurity Maturity Model (C2M2)
- U.S. Department of Homeland Security Industrial Control System Computer Emergency Readiness Team (ICS-CERT)
- Transportation Security Administration Pipeline Security Guidelines, Pipeline Security Smart Practices Observations, and Intermodal Security Training Exercise Program (I-STEP)
- U.S. Coast Guard Maritime Bulk Liquids Transfer (MBLT) Cybersecurity Framework Profile (CFP)

INFORMATION SHARING

The ONG subsector works to share actionable and relevant information across industry, government, and other critical infrastructure partners to build awareness and enable risk-informed decision making. The ONG subsector supports information sharing initiatives through efforts such as:

Information Sharing an Analysis Centers (ISACs) – The ONG subsector is represented by the Downstream Natural Gas ISAC and the Oil and Natural Gas ISAC, which work closely with one another and with other critical infrastructure sector ISACs to share comprehensive analysis of changing threats within the subsector.

Threat Briefings and Workshops – The subsector routinely sponsors and participates in regularly scheduled threat discussions through various means such as calls, briefings, and workshops in an effort to disseminate important, timely information across industry.

OIL AND NATURAL GAS SUBSECTOR COORDINATING COUNCIL

Government Engagement – The ONG subsector engages in voluntary collaboration and information sharing of cyber threat indicators and intelligence with the government at the Federal, State, and Local levels. One such partnership structure is the ONG Subsector Coordinating Council, where 23 ONG trade association representatives and industry management meet with government officials on a regular basis.

Exercises – The ONG subsector participates in cybersecurity exercises with government officials and other critical infrastructure partners to test the subsector preparation and coordination.

Cybersecurity Committees – Most ONG trade associations have committees made up of member companies and cybersecurity professionals that provide briefings and guidance on cybersecurity issues and on proposed legislation.

Peer to Peer Sharing – Through conferences and committees, ONG owners and operators meet regularly to share information and the latest innovations in cybersecurity.

CYBERSECURITY PRACTICES

Security actions being taken by ONG subsector can be described by principles in the *American Gas Association Commitment to Cyber and Physical Security*. At a high-level, each operator evaluates, and implements as appropriate, such principles, 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

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