NATURAL GAS CYBERSECURITY GUIDELINES & STANDARDS PORTFOLIO

Gas utilities and transmission operators apply a myriad of cybersecurity standards, guidelines, and regulatory practices, and tools developed by industry and government entities in their cybersecurity portfolio, as applicable to their individual security environments. These include, but are not limited to:

- American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*
- *AGA Commitment to Cyber and Physical Security* (2016)
- *AGA Cybersecurity Procurement Language Tool*
- *AGA Report 12 – Part I, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*
- AGA and Interstate Natural Gas Association of America (INGAA), *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, (2008)
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-CDV3, *Enterprise-Control System Integration Part 1: Models and Terminology,* (2008)
- ANSI/ISA0-99.00.01-2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models,* (2007)
- ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- American Petroleum Institute (API) & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum & Petrochemical Industries*
- API, *Security Guidelines for the Petroleum Industry*, (2005)
- API, *Standard for Third Party Network Connectivity*, (2007)
- API Standard 1164*, Pipeline SCADA Security*, (2009)
- Center for Internet Security *Critical Security Controls (formerly SANS Top 20 Critical Security Controls)*
- Department of Energy (DOE) ONG Cybersecurity Capability Maturity Model (ONG C2M2)
- DOE *Energy Sector Cybersecurity Framework Implementation Guidance*, (2015)
- DOE Office of Cyber Security, Computer Incident Advisory Capability
- DOE, *21 Steps to Improve Cyber Security of SCADA Networks*
- *DOE Cybersecurity Procurement Language for Energy Delivery Systems*, (2014)
- DHS Control Systems Security Program, *Cyber Security Evaluation Tool* (CSET)
- DHS Chemical Facility Antiterrorism Standards, (2007)
- DHS, *National Infrastructure Protection Plan,* (2013)
- DHS, National Cyber Security Division (NCSD), *Catalog of Control Systems Security: Recommendations for Standards Developers,* (2010)
- DHS NCSD, *Cyber Security Procurement Language for Control Systems Security*, (2009)
- DHS Transportation Security Administration (TSA), *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, (2016)
- *DHS Cybersecurity Questions for CEOs*
- DHS Industrial Control Systems Cyber Emergency Response Team Recommended Practices
- International Organization for Standardization (ISO) and International Electrochemical Commission (IEC), *17799/27001/27002, Information technology - Security techniques - Code of Practice for Information Security Management*
- INGAA, *Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry*, (2011)
- National Association of Regulatory Commissioners Primer, *Cybersecurity for State Regulators* (2017)
- National Institute of Standards and Technology (NIST) SP 800 series
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-82, *Guide to Industrial Control Systems*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity*, (2014)
- North American Electric Reliability Corporation (NERC), NERC-CIP Standards
- TSA *Pipeline Security Guidelines*, (2011)