October 31, 2023

Via Regulations.gov

Ms. Kemba E. Walden
Acting National Cyber Director
Office of the National Cyber Director
The White House

Re: Request for Information: Opportunities For and Obstacles To Harmonizing Cybersecurity Regulations (Docket ID Number: ONCD-2023-0001)

Dear Ms. Walden:

The undersigned trade associations (collectively, the Associations) appreciate the opportunity to provide comments on the Request for Information (RFI) on *Opportunities For and Obstacles To Harmonizing Cybersecurity Regulations*[1]. The Associations represent virtually all aspects of the U.S. oil and natural gas value chain that reliably serve customers across North America. Our members represent refineries and petrochemical companies, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, municipal systems and publicly traded systems, natural gas transmission pipelines, and natural gas product pipelines and processors. As part of the U.S. energy sector that is "uniquely critical due to the enabling functions [it] provide[s] across all critical infrastructure sectors,"[2] the Associations are well-positioned to provide feedback on existing regulatory requirements within the sector, and how a harmonized, outcome-focused, risk-based approach to cybersecurity regulations should be the foundation for any future regulations. The Transportation Security Administration (TSA) embraced such an approach for pipeline cyber security, working in consultation with industry and the Cybersecurity Infrastructure and Security Agency (CISA). This strategy of engagement of has been heralded by the Administration as a prime example of the "collaborative process between industry and regulators" to "produce regulatory requirements that are operationally and commercially viable."[3]

General Comments

The Associations' members understand the importance of regulations to ensure the safe, secure, and reliable provision and delivery of goods and services. However, when cybersecurity requirements conflict, are duplicative, or are overly burdensome, organizations are often left to dedicate key resources to compliance over strengthening, maturing, and advancing their security programs. The herculean effort of harmonizing disparate regulations should be prioritized less with the objective of streamlining oversight, but rather with a focus to understanding the risk within each sector and the myriad of differing purposes for those regulations, be they for national security, safety, or consumer and investor protection.

---

[1] 88 FR 55694 (August 16, 2023).
[2] *Id.*
[3] Biden Administration National Cybersecurity Strategy (March 2023) at p. 8.

Within the energy sector, which encompasses oil, natural gas, and electricity, the objective is to keep energy moving. Therefore, when developing and harmonizing cybersecurity regulations, the federal government should ensure that requirements are risk-informed and are crafted with the objective of protecting those elements critical to ensuring the safe delivery of energy services, protection of personal information, and other necessary functions that support the nation's economy and national security.

At the corporate level, Boards of Directors and senior executives establish the organization's acceptable level of risk mitigation to address all hazards, including cybersecurity threats. An effective cybersecurity program includes continual review to ensure additional resources are dedicated when it is determined that risks need to be addressed and re-affirming the priority of company-wide cybersecurity practices and protocols. To effectively achieve the end goal of robust cybersecurity for critical energy systems, there must be flexibility in the operator's ability to apply risk-informed controls to achieve certain cybersecurity requirements.

Oversight

Oil and natural gas companies have a wide range of government entities with cybersecurity oversight over the same IT or OT systems. For example, existing cybersecurity authorities for the oil and gas sector include: the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Environmental Protection Agency (EPA), the United States Coast Guard (USCG), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Chemical Facility Antiterrorism Standards (CFATS), the Securities and Exchange Commission (SEC), the Nuclear Regulatory Commission (NRC), and state public utility commissions. In addition to the misuse of government and industry resources, there are potential operational complications that multiple reporting regimes can add if they require and audit against different mitigations that cover the same outcome (*e.g.,* different patching timelines in the OT environment). To the extent an oil or natural gas operator is already implementing a preexisting regulatory framework, that should be considered and deemed to satisfy similar requirements in another regulatory program if the same mandated risk reduction outcomes are achieved. In so doing, new requirements would neither compete nor conflict with existing requirements, while constructively introducing regulatory oversight as appropriate.

The Associations likewise urge our federal counterparts to reframe how it views cybersecurity criticality: to move away from the silos of information technology (IT) and operational technology (OT) – as is commonly distinguished now – and instead evaluate based on whether there is impact to the safe and reliable delivery of the commodity or service.

As pipeline safety and pipeline security go hand-in-hand, TSA and the Pipeline and Hazardous Materials Safety Administration (PHMSA) have an existing, and regularly reviewed, Memorandum of Understanding (MoU)[4] that defines the shared responsibility of both agencies to pipeline safety and security, while also clearly distinguishing authorities (*i.e.*, TSA over pipeline security and PHMSA over pipeline safety). The MoU directs the two to coordinate when their actions have the potential for crossover, duplication, or conflict. For example, PHMSA consulted with TSA before issuing updated requirements to operators for sharing detailed pipeline infrastructure information online, citing public access considerations.

[4] https://www.phmsa.dot.gov/about-phmsa/annex-mou-between-phmsa-and-tsa.

It should be recognized that this process is not perfect. In the hasty release of the first iteration of Security Directive Pipeline-2021-02 (SD02A), overly prescriptive mitigation measures including patching cadence, password changes, and other reactive cyber controls were mandated without regard to impact to system operability, product warranties, and patch effectiveness. Proactive controls, such as multi-factor authentication, were required without regard to legacy system capabilities, and rip-and-replace alternatives were directed without consideration to cost or supply chain constraints.

While regulatory reciprocity makes sense for regulations that impact the same operations, assets, or systems, barriers to regulatory reciprocity are primarily due to the silos in which agencies exist. Each agency sees its mission as unique and independent from others. As discussed in greater detail below, the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) attempted to align the regulatory requirements between CISA's CFATS Risk-based Performance Standard (RBPS) 8 (Cybersecurity) and USCG's Maritime Transportation Security Act (MTSA) requirements. During that process, CISA was supportive of this effort while USCG was less amenable to harmonization.

Conflicting, Mutually Exclusive, or Inconsistent Regulations in Oil & Natural Gas

The leading driver of the timely need for cybersecurity regulatory harmonization among federal regulators is the circumvention of duplicative and conflicting requirements, which add an unnecessary administrative burden on the owner/operator and are a waste of scare government resources. This is particularly pertinent given the increasing number of mutually exclusive and inconsistent federal regulations impacting the oil and natural gas sector are often even within single federal departments. As alluded, within DHS alone, TSA, CISA, and USCG all have a regulatory role related to cybersecurity within various segments of the oil and natural gas supply chains. While not necessarily conflicting, especially at the federal level, these regulations are certainly duplicative, burdensome from a compliance perspective, and are inconsistently enforced.

TSA

TSA has issued two Pipeline Security Directives (SDs), currently on versions Security Directive Pipeline 2021-01C[5] (SD-01C) and Security Directive Pipeline 2021-02D[6] (SD-02D), as the agency works towards releasing a Notice of Proposed Rulemaking (NPRM), related to pipeline and liquified natural gas (LNG) facilities' cybersecurity processes.

SD-01C requires covered pipeline and LNG facilities to report cybersecurity incidents to CISA; designate a cybersecurity coordinator available to TSA and CISA at all times for the purpose of coordinating with the agencies in the event of a cybersecurity incident; and review their current activities against TSA pipeline cybersecurity recommendations to assess cyber risks, identify gaps, develop remediation measures, and report those results to TSA and CISA.

SD-02D requires covered pipeline and LNG facilities to establish and implement a TSA-approved Cybersecurity Implementation Plan (CIP) outlining specific cybersecurity measures, along with a schedule for meeting outcomes designated by TSA; develop and keep current a Cybersecurity Incident Response Plan (CIRP) aligned with TSA requirements; develop and submit for TSA-approval a Cybersecurity Assessment Plan detailing how the effectiveness of their cybersecurity measures will be assessed and how

[5] *See* https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01c.pdf (May 29, 2023).
[6] *See* https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf (July 27, 2023).

vulnerabilities will be identified and resolved; and submit an annual report describing their Cybersecurity Assessment Plan (CAP) results from the prior year.

It remains to be seen how the NPRM TSA plans to release later this year will dovetail with these existing requirements.

CISA

CISA's CFATS[7] program requires any facility that manufactures, uses, stores, or distributes chemicals of interest (COIs) at or above a screen threshold quantity to report those holdings to CISA within 60-days of coming into possession of those chemicals. High-risk, tiered facilities are also required to submit a Security Vulnerability Assessment and a Site Security Plan, or an Alternative Security Program, that meets 18 defined RBPS[8] intended to address security issues, including cybersecurity[9]. Prior to Congress' recent failure to reauthorize the CFATS program, CISA was in the process of developing an NPRM expected to include additional cybersecurity requirements for covered facilities.

USCG

Oil and natural gas facilities regulated by the USCG under MTSA[10] are similarly required to assess, document, and remediate computer system or network vulnerabilities in their Facility Security Assessments (FSAs) submitted to the USCG, and document how those vulnerabilities have been addressed in the required Facility Security Plans (FSPs). The USCG is also in the process of developing an NPRM related to cybersecurity requirements for these regulated facilities.

Harmonizing Existing Disparate Requirements

Each of the regulatory requirements described above are administered by agencies under the purview of a single federal department, DHS. However, little effort has been made to harmonize even these efforts, leading to increased administrative burdens for covered entities in coordinating with, and meeting the requirements of, these respective agencies. Further, as mentioned, effort by the ONG SCC to pilot the harmonization of the cyber assessments of CISA and the USCG. Though both entities welcomed the concept of harmonization, neither would concede their own approach to implement the harmonized approach.

If proactive efforts cannot be made to harmonize or rectify the disparate requirements placed upon owners/operators when developing cybersecurity regulatory requirements, agencies would be well served to take action to retroactively ensure that regulatory requirements applicable to entities regulated by multiple agencies are harmonized in a reciprocating manner. Doing so would reduce the regulatory burden on industry owners and operators and would allow the federal agencies administering these requirements to streamline their efforts.

When considering new cybersecurity regulatory requirements, we encourage regulators to consult with other existing regulatory bodies with authorities in a respective sector as well as with regulators of other sectors with direct ties to the sector for which cybersecurity regulations are under development, (*e.g.*, oil and natural gas subsector has ties with chemical, transportation, electric, water, nuclear, dams,

[7] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats.
[8] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-risk-based-performance-standards.
[9] *See* https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-risk-based-performance-standards-rbps/rbps-8-cyber.
[10] 46 U.S.C. Chapter 701 (2002).

telecommunications, and other sectors). It is critical that any new requirements are harmonized with existing regulations to ensure there are no unintended consequences or impacts to reliable, safe operations. For example, in early iterations of the TSA Pipeline Security Directives, TSA promulgated prescriptive regulations without a consultative process. This resulted in mitigation measures that not only posed a risk to operational safety but also, in some cases, were impossible to achieve within the pipeline environment.

Federal agencies considering cybersecurity regulations should leverage the lessons learned and proactively discuss how their proposals may impact existing regulations in the safety, security, and operational space. The more the federal government is able to consistently develop and apply regulations, the more operators will be able to understand and implement those requirements, definitions, and objectives, which will allow them to focus more effectively on addressing cyber threats and mitigations.

When mandated to comply with prescriptive requirements, substantial additional time and effort should be expected in the resource analysis. While this may not be seen on the surface as a setback, resource diversion often halts timely corporate initiatives on other cyber capital improvements. The cost of compliance may be even more impactful for those operators with less resources. Since operators take a risk-based, corporate approach to managing the security of their assets, future regulations *must* address prohibitive costs and support outcome-focused, flexible requirements that allow organizations to manage risks in a way that is efficient and effective for the uniquities of their systems.

Toward this end, we would also encourage ONCD to consider whether a single entity, such as CISA, could play the harmonizing role to ensure consistent standards and requirements across jurisdictions covering cybersecurity. Different regulators with various requirements create redundancies, which increases the risk for potential cybersecurity gaps. A single entity to provide management and oversight of the myriad of cybersecurity regulations would enhance overall cybersecurity and ease compliance efforts. A simplified analogy would be for CISA to serve as a "traffic cop" to which all cybersecurity requirements for critical infrastructure sectors must pass by and ensure alignment with existing as appropriate. CISA could rely on a clearinghouse containing all existing requirements. New cybersecurity regulation would go through the clearinghouse to ensure it is (a) aligned with existing requirements from the federal government, and (b) is not duplicative with existing requirements on a sector/tangential sector.

Use of Existing Standards or Frameworks in Oil & Natural Gas

Conflicting requirements occur when regulatory bodies seek prescriptive measures. If the requirements are risk-based and outcome-focused, then even divergent requirements converge when the common outcome is achieved. Effective cyber risk management cannot be implemented in a vacuum; it *must* be part of an overall risk management program. Oil and natural gas companies leverage a diverse portfolio of cyber and risk management frameworks, standards, and guidelines to their individual cyber programs to be suitable to their unique operational environments. These approaches are driven by many factors, including but not limited to, threat-informed analysis, operating safety, regulatory requirements, and fiduciary responsibility. The following is a non-exhaustive list of references from oil and natural gas federal regulators and non-regulators from the oil and natural gas sector[11]:

- API 1164
- CFATS RBPS 8

[11] *See* Appendix A for standards, frameworks, and guidance acronyms.

- CIS Best Practices Guidelines
- ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems Security
- ISO/IEC 27000 family of ISO/IEC ISMS standards
- ISO 31000 Risk Management
- CISA CPGs
- CISA Best Practice and Implementation Guides, advisories, alerts
- DOD CMMC
- DOE C2M2
- FAIR Quantitative Model for Information Security and Operational Risk
- NERC CIP
- NIST: CSF v1.1; Risk Management Framework series; and associated NIST guidance publications including 800-53 R5 and 800-82 R3
- SANS Frameworks
- SOX
- TSA PSGs
- USCG Guidance

In recent years, the Oil & Natural Gas Subsector Coordinating Council (ONG SCC) has been actively working towards a master cyber assessment that overlays all current cyber regulations, standards, and frameworks, and identifies the areas of overlap. Those areas would be incorporated into this cyber assessment, comparable to or possibly building off CISA's Cyber Security Evaluation Tool (CSET)[1]. Each federal agency could have an appendix to the cyber assessment that addresses requirements specific to that sector/industry.

The security and pipeline safety regulators in the oil and natural gas industry understand, or are at least aware of, the standards and frameworks listed above. For example, API STD 1164 v3[12] is a conglomeration of many of the listed standards/frameworks, and representatives from TSA, the FERC, the Department of Energy (DOE), and DHS participated in the development of API 1164 v3. Still, just as there is no single standard or framework that suits every critical infrastructure sector uniformly, there is no single standard or framework that suits every oil and natural gas operation in the same way. For instance, some operators of natural gas companies that deliver both natural gas and electric may apply portions of NERC CIP to their natural gas operations. This should not be misconstrued to mean NERC CIP is applicable in the same manner across all operators of natural gas.

Nonetheless, the responsibility to demonstrate conformity with existing standards or frameworks belongs to the operators. The responsibility to audit and verify compliance with any regulatory requirements that reference existing standards or frameworks belongs to the government. The methodologies used by the government to verify compliance is where the challenge lies. If the government seeks to audit efficiency over effectiveness, then operators are most often driven to a prescriptive, one-size-fits-all model measured solely by check-the-box compliance. However, compliance does not equate to operational security. If the government seeks efficacy within security, then operators should be accountable for following and maturing a risk-based program that is measured through a standardized audit process.

The Associations' members utilize various types of assessments across their IT and OT networks. The use of assessments is based on business and operational needs that change over time and as technologies change within an operation. Some assessments may take more time to plan or may have different risks that need to be addressed. For instance, penetration testing may be appropriate for an IT environment but could be incredibly disruptive in the OT environment. IT assessments may optimize and create efficient IT systems in order to decrease costs, reduce risk, and improve governance and security, while a

[12] *See* https://www.api.org/products-and-services/standards/important-standards-announcements/1164.

vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed. The business case will vary across a company's operations and networks and will inform the schedule and frequency of a particular assessment.

Third-Party Frameworks

There are many paths to develop a robust and effective cybersecurity program, and oil and natural gas companies implement diverse types of cybersecurity programs that can comprise many components. Based on the organization's risk profile, oil and natural gas owners/operators orient their IT and OT cybersecurity programs to various leading frameworks and best-in-class standards, most commonly the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[13] and the International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security[14]. API, through an American National Standards Institute-approved consensus process, has also developed several voluntary standards that can be used across the industry. This consensus-based process involves operators, regulators, vendors, and others that have material interest in the subject.

API Standard (STD) 1164 v3[15], *Pipeline Control Systems Cybersecurity*, was created through several years of dedicated work by a broad coalition of stakeholders, including DHS, DOE, and TSA, and was published in August of 2021. This voluntary standard builds on the NIST CSF, as well as the ISA/IEC 62443 series of standards, and provides requirements and guidance for managing cyber risk associated with infrastructure as code (IaC) environments to achieve security, integrity, and resiliency objectives. Furthermore, in 2023, DHS designated and certified API STD 1164 as a Qualified Anti-Terrorism Technology (QATTs) under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, also known as the SAFETY Act, highlighting its effectiveness in aiding oil and natural gas entities in ensuring a strong and effective cybersecurity posture.[16]

We recommend that any effort to harmonize cybersecurity regulation rely on performance-based mechanisms, including proven frameworks and public-private collaboration, rather than prescriptive standards or regulations, is the most effective means to bolster the cybersecurity of natural gas and oil systems and to afford the necessary flexibility and agility to respond to a constantly changing cyber threat landscape. Prescriptive measures can restrain a company's ability to respond to changing threats in a nimble and responsive way, while establish frameworks are well understood and allow operators to tailor their response to the specific threat.

Another set of resources is the DOE Cybersecurity Capability Maturity Model (C2M2) which helps operators evaluate their own cybersecurity programs and can provide benchmarking for an operator to allow for continuous improvement. C2M2 was developed by DOE with input from a variety of operators across the energy sector and has been in use since 2012. For the past several years, TSA, in partnership with CISA and Idaho National Laboratory (INL), has also been providing Validated Architecture Design Reviews (VADR), a process also built on the NIST CSF as part of their structured pipeline security oversight

[13] *See* https://www.nist.gov/cyberframework.
[14] *See* https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
[15] *See* https://www.api.org/products-and-services/standards/important-standards-announcements/1164.
[16] *See* https://www.dhs.gov/science-and-technology/safety-act.

program. The VADRs, "provide the owners and operators of pipeline infrastructure with a comprehensive evaluation and discovery process, while simultaneously focusing on the best defense strategies associated with asset owners' specific control systems network."[17] While some operators utilize portions of the recently published Cybersecurity Performance Goals (CPGs)[18], the CPGs as released conflict with select measures in the TSA Security Directives, despite attention drawn to such conflicts in the CPG Check List[19].

As mentioned above, the Associations' members likewise utilize various voluntary methodologies to assess physical and cyber risk to the operational environment. Two related methodologies are API Recommended Practice (RP) 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries[20], and API RP 781, Facility Security Plan Methodology for the Oil and Natural Gas Industries[21]. Combined, these two recommended practices provide the tools and flexibility for operators to tailor assessments and plans to the individual facilities and operations to protect people, assets, and operations. In addition, API has API RP 1168, Pipeline Control Room Management, Second Edition[22], provides pipeline operators and controllers with guidance on industry best practices for control room management when developing or enhancing processes, procedures, and training.

Other voluntary standards, such as API RP 1173, Pipeline Safety Management Systems,[23] support operator's pipeline safety management systems (PSMS) and provides pipeline operators with safety management system requirements that, when applied, provide a framework to reveal and manage risk, promote a learning environment, and continuously improve pipeline safety and integrity. Operators also might utilize the third edition of API RP 1160, Managing System Integrity for Hazardous Liquid Pipelines,[24] which provides a process for establishing safe pipeline operations, including robust assessments of potential risks and establishment of systems to manage them safely and sustainably throughout day-to-day operations. Additional PHMSA regulations, such as the Operator Qualification (OQ) rule,[25] require each pipeline operator to develop an OQ program, follow their written OQ plan, establish a covered task list applicable to their system, and define the training and qualification requirements for personnel performing covered tasks on their pipeline facility. These resources create and bolster the security of OT operations, systems, and facilities, and help mitigate cyber risk.

In summary, there are ample credible and operator-tested third-party frameworks that can be leveraged for harmonization. The key is recognizing not one single framework fits all critical infrastructure sectors equally.

Defense-In-Depth Rather Than Tiered Regulation

---

[17] *See* https://www.cisa.gov/sites/default/files/publications/19_0305_cisa_pipeline-cybersecurity-initiative-factsheet
pdf

[18] *See* https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[19] *See* https://www.cisa.gov/sites/default/files/publications/CISA_CPG_CHECKLIST_508c.pdf.

[20] *See* https://www.api.org/~/media/files/publications/whats%20new/780%20e1%20pa.pdf.

[21] *See* https://www.apiwebstore.org/standards/781.

[22] *See* https://www.api.org/~/media/files/publications/whats%20new/1168_e2%20pa.pdf.

[23] *See* https://www.api.org/~/media/files/publications/whats%20new/1173_e1%20pa.pdf.

[24] *See* https://www.api.org/products-and-services/standards/important-standards-announcements/recommended-practice-1160.

[25] Subpart N in 49 CFR Part 192 and Subpart G in 49 CFR Part 195.

Oil and natural gas operators apply risk-based "defense-in-depth" approaches to cybersecurity just as they use it to manage other enterprise risks such as safety hazards, changes in laws or regulations, geopolitical forces, changes in market demand or competition, or other systemic financial risks. The impact of any of these risks will vary by the time of year, region of the U.S., and among different system resiliencies.

Defense-in-depth is a layered approach to security to provide maximum protection against threats. Defense-in-depth layers include physical and network security, administrative, antivirus, and behavioral controls. This approach entails robust governance, systematic risk-based management, and multi-dimensional programs based on industry-recognized standards and proven frameworks. These defense-in-depth approaches are based on the organization's risk acceptance. The industry paper *Defense-in-Depth: Cybersecurity in the Natural Gas & Oil Industry,*[26] as quoted here, details the industry's typical approach:

> *Regardless of the structure used for cybersecurity program development, natural gas and oil companies typically buffer ICS from cyberattacks through the use of "defense-in-depth" network architecture. Natural gas and oil companies segment their systems and implement "demilitarized zones" (DMZ) between industrial controls and internet facing business networks.*

CISA's CFATS program has a relatively effective risk-based tiered approach: as a facility increases in tier, the operator has more responsibilities and risks to consider. The functional word is "consider." Given the lack of uniformity across all critical infrastructure sectors and even across a single sector (*e.g.*, the energy sector encompasses oil, natural gas, and electricity), tiers accompanied by prescriptive measures and without consideration to impact and resilience would incapacitate the owner/operator. Consequently, any such tiering approach to regulation must be scoped thoughtfully and with transparency.

Conclusion

Managing compliance obligations with disparate regulations and agencies may in fact harm the cybersecurity posture of organizations, particularly where limited resources are allocated to compliance activities over managing risk, maturing capabilities, and creating effective security programs. Ensuring efficient and appropriate regulatory regimes that are harmonized and streamlined in order to ensure that organizations are able to focus on hardening their defenses is a top priority for the Associations and its members. We appreciate the opportunity to provide comments on this RFI and look forward to future engagement throughout the rulemaking process.

Sincerely,

American Fuel & Petrochemical Manufacturers Association (AFPM)

American Gas Association (AGA)

American Petroleum Institute (API)

Interstate Natural Gas Association of America (INGAA)

[26] *See* https://www.api.org/-/media/files/policy/cybersecurity/2018/defense-in-depth-cybersecurity-in-the-natural-gasand-oil-industry.pdf

Appendix A: Standards, Frameworks, and Guidance Acronyms

- American Petroleum Institute (API) 1164
- Chemical Facility Antiterrorism Standards Risk-Based Performance Standard (CFATS RBPS) 8
- Center for Internet Security (CIS) Best Practices Guidelines
- International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443 Series of Standards on Industrial Automation and Control Systems Security
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 family of ISO/IEC Information Security Management Systems (ISMS) standards
- International Organization for Standardization (ISO) 31000 Risk Management
- Cybersecurity and Infrastructure Security (CISA) Cybersecurity Performance Goals (CPGs)
- Cybersecurity and Infrastructure Security (CISA) Best Practice and Implementation Guides, advisories, alerts
- Department of Defense Cybersecurity Maturity Model Certification (DOD CMMC)
- Department of Energy Cybersecurity Capability Maturity Model (DOE C2M2)
- Factor Analysis of Information Risk (FAIR) Quantitative Model for Information Security and Operational Risk
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- National Institutes of Standards and Technology Cybersecurity Framework (NIST CSF) v1.1; Risk Management Framework series; and associated NIST guidance publications including 800-53 R5 and 800-82 R3
- Escal Institute of Advanced Technologies (SANS) frameworks
- Sarbanes Oxley (SOX)
- Transportation Security Administration Pipeline Security Guidelines (TSA PSGs)
- United States Coast Guard (USCG) Guidance