

TSA Pipeline Cyber Security Measures - Baseline

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 6.3 Site-Specific Security Measures. Requirements are centered around physical protection of facilities.

Revision Date	Assessment Type
21 Jun	Compliance
# Questions	Complexity/Level of
47	Low
Industries Used By	Energy, Oil & Gas

DFARS 800-171 Assessment

Defense Federal Acquisition Regulation Supplement. Assesses data safeguarding standards required for all Department of Defense (DOD) contractors. Based on Rev 2 DoD requirements from NIST 800-171 .

Revision Date	Assessment Type
20 Jan	Compliance
# Questions	Complexity/Level of
110	Low
Industries Used By	All sectors supporting the DOD

Australian Energy Sector Cyber Security Framework (AESCFS)

For Australian energy companies. Derived from the May 2021 Framework Core. Contains Australian-specific controls, along with questions from existing frameworks, such as the United States' ES-C2M2 and NIST-CSF.

Revision Date	Assessment Type
21 May	Compliance
# Questions	Complexity/Level of
282	Medium
Industries Used By	Energy, Power Utility

20

Industry Frameworks Available

16

Critical Infrastructure Sectors Covered

3,089

Cybersecurity Control Questions

+Module Builder

Bring your framework, Create a framework, Customize a standard framework

C2M2-Electric

Electricity Subsector Cybersecurity Capability Maturity Model. Evaluates cybersecurity posture of organizations within the energy sector.

Revision Date	Assessment Type
19 Oct	Compliance
# Questions	Complexity/Level of
315	Medium
Industries Used By	Energy, Power Utility

C2M2-Oil & Gas

Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model. Evaluates cybersecurity posture; specific to oil & gas organizations, based on ES-C2M2

Revision Date	Assessment Type
19 Oct	Compliance
# Questions	Complexity/Level of
315	Medium
Industries Used By	Energy, Oil & Gas

SOC 2: TSP - 2017

SOC2: Trust Services Criteria evaluates security, availability, processing integrity, confidentiality, and privacy compliance controls for service organizations.

Revision Date	Assessment Type
18 Dec	Compliance
# Questions	Complexity/Level of
61	Low
Industries Used By	All critical infrastructure sectors

Critical Infrastructure Maturity Model (CIMM) V2.0

Guides organizations in understanding the maturity of their cyber risk program.

Revision Date	Assessment Type
21 Nov	Maturity
# Questions	Complexity/Level of
17	Low
Industries Used By	All critical infrastructure sectors

NIST 800-53 Rev. 5

This NIST special publication provides a catalog of security and privacy controls for information systems and organizations from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

Revision Date	Assessment Type
21 Jun	Compliance
# Questions	Complexity/Level of
298	Medium
Industries Used By	All critical infrastructure sectors

TSA Pipeline Site-Specific Measures - Baseline

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 6.3 Site-Specific Security Measures, requirements are centered around physical protection of facilities. These measures should be tailored explicitly for each facility and address specific actions to be taken in response to pertinent NTAS Bulletins or Alerts.

Revision Date	Assessment Type
21 Jun	Compliance
# Questions	Complexity/Level of
31	Low
Industries Used By	Energy, Oil & Gas

TSA Pipeline Site-Specific Measures - Baseline + Enhanced

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 6.3 Site-Specific Security Measures, requirements are centered around physical protection of facilities. These measures should be tailored explicitly for each facility and address specific actions to be taken in response to pertinent NTAS Bulletins or Alerts.

Revision Date	Assessment Type
21 Jun	Compliance
# Questions	Complexity/Level of
62	Low
Industries Used By	Energy, Oil & Gas

TSA Pipeline Cyber Security Measures - Baseline + Enhanced

Based on TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), 7.3 Security Measures for Pipeline Cyber Assets, requirements are centered around protection of facilities against cyber threats.

Revision Date	Assessment Type
21 Jun	Compliance
# Questions	Complexity/Level of
59	Low
Industries Used By	Energy, Oil & Gas

SG OT Cyber Maturity

Evaluates an entity's OT environment. Based on NIST 800-53 and IEC 62443.

Revision Date	Assessment Type
18 Nov	Compliance
# Questions	Complexity/Level of
151	Low
Industries Used By	All critical infrastructure sectors with industrial operations

SG IT Cyber Maturity

Evaluates an entity's IT environment, based on NIST 800-53 and ISO 27001/2.

Revision Date	Assessment Type
18 Nov	Maturity
# Questions	Complexity/Level of
122	Low
Industries Used By	All critical infrastructure sectors

NERC CIP

Compliance standard for the reliability and security of the Bulk Electric System of North America.

Revision Date	Assessment Type
20 Dec	Compliance
# Questions	Complexity/Level of
135	High
Industries Used By	Energy, Power Utility

NIST Cybersecurity Framework (CSF)

Evaluates adherence to NIST cybersecurity standards and best practices

Revision Date	Assessment Type
19 Oct	Compliance
# Questions	Complexity/Level of
108	Low
Industries Used By	All critical infrastructure sectors

General Data Protection Regulation (GDPR)

Data protection and privacy compliance to the European Union & European Economic Area General Data Protection Regulation.

Revision Date	Assessment Type
21 Aug	Compliance
# Questions	Complexity/Level of
365	High
Industries Used By	All critical infrastructure sectors

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity Maturity Model Certification. Evaluates handling of CUI for a Defense Industrial Base contractor. It consists of 171 practices that are mapped across five levels.

Revision Date	Assessment Type
20 Jul	Maturity
# Questions	Complexity/Level of
171	Medium
Industries Used By	All sectors supporting the DOD

NIST 800-82 Section 6.2

Evaluates performance against the SP 800-53 control families and implementation considerations for ICS owners.

Revision Date	Assessment Type
18 Nov	Compliance
# Questions	Complexity/Level of
86	Low
Industries Used By	All critical infrastructure sectors with industrial operations

Rev. 3 COMING SOON

Maritime

Vessel/entity compliance based on both BIMCO and IMO guidelines.

Revision Date	Assessment Type
19 Jun	Compliance
# Questions	Complexity/Level of
354	High
Industries Used By	Energy, Oil & Gas, Transportation, Defense