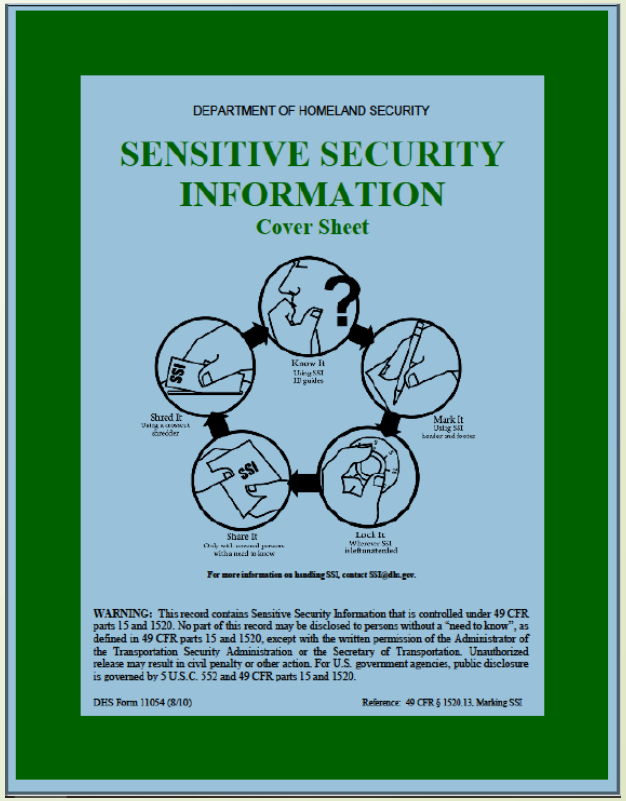
TSA Pipeline Cybersecurity Self-Assessment

OMB Control Number 1652-0050

Exp. 11/31/2021

When completed, this document is SSI.



DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet

For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

OMB 1652-0050
Exp. 11/30/2021

Transportation Security Administration

U.S. Department of Homeland Security

Revised: 05/XX/2021

TSA Pipeline Cybersecurity Self-Assessment

Owner/Operator Name:		Assessment Completed Date:	
		TSA's Pipeline Security Guidelines Sect.7 Review Date:	
Submitter (First/Last):		Submitter Title:	
Submitter Email:		Submitter Contact Number:	
Cybersecurity Coordinator (First/Last):		Cybersecurity Coordinator Title:	
Cybersecurity Coordinator Email:		Cybersecurity Coordinator Contact Number:	

Instructions: Select the appropriate response for each question below. Additional information may be added within the shaded boxes. For any questions concerning the completion of this assessment please email SurfOps-SD@tsa.dhs.gov.

Question #	Question	Answer (Yes/No)	Additional Information
Pipeline Cyber Asset Security Measures			
1.00	Do your cybersecurity plans incorporate any of the following approaches?		
1.00A	National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity	<Select>	
1.00B	U.S. Department of Energy, Office of Electricity and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance	<Select>	
1.00C	U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance	<Select>	
1.00D	Industry-specific methodologies (See 2018 TSA Pipeline Security Guidelines, Section 7.4 for partial listing.)	<Select>	
1.00E	Other (if checked, elaborate)	<Select>	
Asset Management			

2.00	Has your corporation established and documented policies and procedures for the following?		
2.00A	Assessing and maintaining configuration information.	<Select>	
2.00B	Tracking changes made to pipeline cyber assets.	<Select>	
2.00C	Patching/upgrading operating systems and applications.	<Select>	
2.00D	Ensuring that the changes do not adversely impact existing cybersecurity controls.	<Select>	
2.00E	Other (if checked, elaborate)	<Select>	
2.01	Does your corporation evaluate and classify pipeline cyber assets using the following criteria?		
2.01A	Critical pipeline cyber assets are operational technologies (OT) systems that can control operations on the pipeline.	<Select>	
2.01B	Non-critical pipeline cyber assets are OT systems that monitor operations on the pipeline.	<Select>	
2.02	Has your corporation developed and maintained a comprehensive setof network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows?	<Select>	
2.03	For critical pipeline cyber assets, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints?	<Select>	
2.04	For critical pipeline assets, has an inventory of the components of the operating system been developed, documented, and maintained that accurately reflects the current OT system?	<Select>	

2.05	For critical pipeline cyber assets, does your corporation review network connections periodically, including remote access and third-party connections?	<Select>	
2.06	For critical pipeline cyber assets, has your corporation implemented the following measures?		
2.06A	Restrict user physical access to control systems and control networks by using appropriate controls.	<Select>	
2.06B	Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).	<Select>	
2.07	For critical pipeline cyber assets, does your corporation review, assess, and update as necessary all cybersecurity policies plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational change?	<Select>	
2.08	Does your corporation review and assess pipeline cyber asset classification as critical or noncritical at least every 12 months?	<Select>	
Business Environment			
3.00	Does your corporation have a designated individual solely responsible for cyber/SCADA security?	<Select>	
3.01	Does your corporation ensure that any change that adds control operations to a non-critical pipeline cyber asset results in the system being recognized as a critical cyber pipeline asset and enhanced security measures being applied?	<Select>	
Governance			
4.00	Does your corporation have a designated individual solely responsible for cyber/ IT/ OT / SCADA security?	<Select>	
4.01	Has your corporation established and distributed cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment?	<Select>	

4.02	Is your company formally addressing ALL 2018 Pipeline Security Guidelines cyber security measures detailed in Section 7 of the Guidelines and formally detailing these measures in overarching corporate security and IT/OT security plans?	<Select>	
4.03	Does your corporation review, assess, and update as necessary all cybersecurity policies plans, processes, and supporting procedures at least every 36 months, or when there is a significant organizational or technological change?	<Select>	
	Risk Management Strategy		
5.00	Has your corporation developed an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks?	<Select>	
	Risk Assessment		
6.00	For critical pipeline cyber assets, does your corporation use independent assessors to conduct pipeline cybersecurity assessments?	<Select>	
6.01	Has your corporation established a process to identify and evaluate vulnerabilities and compensating security controls?	<Select>	
6.02	Does the process address unmitigated/accepted vulnerabilities in the IT and OT environment?	<Select>	
	Access Control		
7.00	Has your corporation implemented the following measures?		
7.00A	Establish and enforce unique accounts for each individual user and administrator.	<Select>	
7.00B	Establish security requirements for certain types of privileged accounts.	<Select>	
7.00C	Prohibit the sharing of these accounts.	<Select>	
7.01	Are authentication methods and specific standards such as strong credential management, Active Directory monitoring, employed throughout your company's cyber access control environment and	<Select>	

7.02	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?	<Select>	
7.03	Does your corporation ensure user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company?	<Select>	
7.04	Has your corporation implemented the following measures?		
7.04A	Establish and enforce access control policies for local and remote users.	<Select>	
7.04B	Have procedures and controls in place for approving and enforcing remote and third-party connections.	<Select>	
7.05	Are access control levels of permission and privileges defined in the IT/ OT security plan?	<Select>	
7.06	Does your corporation ensure appropriate segregation of duties is in place and, where this is not feasible, apply appropriate compensating security controls?	<Select>	
7.07	Does your corporation change all default passwords for new software, hardware, etc., upon installation and, where this is not feasible (e.g., a control system with a hard-wired password), implement appropriate compensating security controls (e.g., administrative controls)?	<Select>	
7.08	Do email and communications systems have features that automatically download attachments turned off?	<Select>	
7.09	Do systems only allow the execution of programs known and permitted by security policy (i.e., whitelist or allow lists?)	<Select>	
Awareness & Training			
8.00	Do all persons requiring access to the company's pipeline cyber assets receive cybersecurity awareness training?	<Select>	

8.01	For critical pipeline cyber assets, does your corporation provide role-based security training on recognizing and reporting potential indicators of system compromise prior to granting access to critical pipeline cyber assets?	<Select>	
8.02	Is there a cyber-threat awareness program for employees that includes practical exercises/testing?	<Select>	
Data Security & Information Protection			
9.00	Has your corporation established and implemented policies and procedures to ensure data protection measures are in place, including the following?		
9.00A	Identifying critical data and establishing classification of different types of data.	<Select>	
9.00B	Establishing specific data handling procedures.	<Select>	
9.00C	Establishing specific data disposal procedures.	<Select>	
Protective Technology			
10.00	Are pipeline cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections?	<Select>	
10.01	Do IT/ OT systems monitor and manage communications at appropriate IT/ OT network boundaries?	<Select>	
10.02	Does your corporation employ mechanisms (e.g., active directory) to support the management of accounts for critical pipeline cyber assets?	<Select>	
10.03	Does your corporation regularly validate that technical controls comply with the company's cybersecurity policies, plans, and procedures, and report results to senior management?	<Select>	
10.04	Has your corporation implemented technical or procedural controls to restrict the use of pipeline cyber assets to only approved activities?	<Select>	
Anomalies & Events			

11.00	Has your corporation implemented processes to respond to anomalous activity through the following?		
11.00A	Generating alerts and responding to them in a timely manner.	<Select>	
11.00B	Logging cybersecurity events and reviewing these logs.	<Select>	
Security Continuous Monitoring			
12.00	Does your corporation monitor for unauthorized access or the introduction of malicious code or communications?	<Select>	
12.01	Does your corporation monitor physical and remote user access to critical pipeline cyber assets?	<Select>	
12.02	For critical pipeline cyber assets, does your corporation employ mechanisms to detect unauthorized components?	<Select>	
12.03	Does your corporation conduct cyber vulnerability assessments as described in your risk assessment process?	<Select>	
Detection Processes			
13.00	Has your corporation established technical or procedural controls for cyber intrusion monitoring and detection?	<Select>	
13.01	Does your corporation perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?	<Select>	
Response Planning			
14.00	Has your corporation established policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams?	<Select>	
14.01	For critical pipeline cyber assets, are cybersecurity incident response exercises conducted periodically?	<Select>	
14.02	For critical pipeline cyber assets, has your corporation established and maintained a process that supports 24/7 cyber-incident response?	<Select>	

14.03	Has your corporation established and maintained a cyber-incident response capability?	<Select>	
Communications			
15.00	Does the corporation have procedures in place for reporting to CISA Central (formerly the National Cybersecurity and Communications Integration Center (NCCIC)) in accordance with SD Pipeline 2021-01 for actual or suspected cyber-attacks that could impact pipeline industrial control systems (SCADA, PCS, DCS) measurement systems and telemetry systems or enterprise-associated IT systems? (Appendix B – TSA Notification Criteria, 2018 TSA Pipeline Security Guidelines.)	<Select>	
Mitigation			
16.00	Do your corporation's response plans and procedures include mitigation measures to help prevent further impacts?	<Select>	
Recovery Planning			
17.00	Has your corporation established a plan for the recovery and reconstitution of pipeline cyber assets within a time frame to align with the company's safety and business continuity objectives?	<Select>	
17.01	Does the company have documented procedures in place to coordinate restoration efforts with internal and external stakeholders (coordination centers, Internet Service Providers, victims, vendors, etc.)?	<Select>	
Continuous Improvement			
18.00	Does your corporation review its cyber recovery plan annually and update it as necessary?	<Select>	

Submit information to:
There are two methods to submit this TSA Pipeline Cybersecurity Self-Assessment as the information is considered Sensitive Security Information (SSI) once completed.

The first is via email and a password protected document with the password being sent in a separate email to: SurfOps-SD@tsa.dhs.gov. Please refer to SD FAQs for SSI password requirements.

The second is to upload the document on a specific secure portal that TSA has established on HSIN-CI under the ONG subsector. File name format for submission via either method should be as follows: "Operator Name-TSA SD Assessment-MMDDYYYY", where the date is date of submission. If you do not have access to HSIN, please contact SurfOps-SD@tsa.dhs.gov for assistance.

Paperwork Reduction Act Statement

- **PAPERWORK REDUCTION ACT STATEMENT**: TSA is collecting this information in order to address cybersecurity threat to pipeline systems and associated infrastructure. This is a mandatory collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 6 hours. If you have any comments regarding this form, you may write to: ATTN: TSA PRA Officer, TSA-11, PRA 1652-0050, 6595 Springfield Center Drive, Springfield, VA 20598-6011. An agency may not conduct or sponsor, and persons are not required to respond to, a collection of information unless it displays a currently valid OMB control number. The OMB number for this for is 1652-0050, which expires 11/31/2021.