DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION
Cover Sheet

Know It
Using SSI
ID guides

Mark It
Using SSI
header and footer

Lock It
Wherever SSI
is left unattended

Share It
Only with covered persons
with a need to know

Shred It
Using a crosscut
shredder
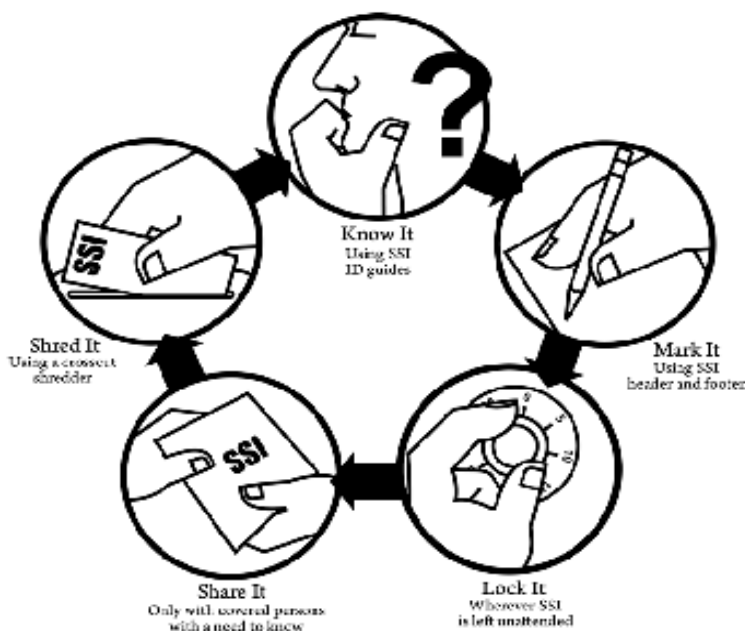
For more information on handling SSI, contact SSI@dhs.gov.

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

DEPARTMENT OF HOMELAND SECURITY		
Transportation Security Administration		

Pipeline Corporate Security Review (CSR)	**CSR FY2020 V.1 (October 2019)**

Please enter letter airport your field of assignment.

	CSR Date	TSA Field Office
	1/1/2019	**N/A (SSI - Contractor)**
	Report Date	HTUA Name
		<Please Select>

TYPE OF VISIT	**Name of Pipeline Operator**		
Corporate Security Review			

Is This A Revisit?	**Date of Previous CSR?**	**Street**	
		County	

		City		**State**		**Zip Code**	

Corporation / Company Mailing Address

US States of Operation (List):	**Street**				
	City		**State**	**Zip Code**	

International Cross-border Operations (Y/N):		**Agency Website:**	

24-Hour Emergency Contact Telephone Numbers			**Employees**	
Purpose	**Telephone**		Total Corporate Employees	
1	**24-Hour Emergency**		Total Pipeline Operations Employees	
2			**Product Flow**	
3			Number of pipeline systems operated	

Products Carried (mark applicable with "X"):			Total Pipeline Mileage	
< Natural Gas/LNG		< Crude Oil	Pipeline size(s)	
< Refined Products		< NGL/LPG	Maximum daily flow capacity	
< Toxic Inhalation Hazard (TIH)			Average daily flow capacity	
< Chemicals (list below)			Annual Deliveries	
List >			Storage Capacity	

Infrastructure Inventory

Quantity	Infrastructure	Quantity	Infrastructure
	Pipelines on Bridges		NGL Facilities
	Standalone Pipeline Bridges		Marine Terminals
	Storage Facilities		SCADA Control Rooms
	Breakout Tank Facilities		Backup SCADA Control Rooms
	Pumping Stations		Emergency Operations Centers
	Compressor Stations		Delivery Points
	LNG Facilities		Other

Corporation / Company Profile Comments:

Comments:

Security Personnel Interviewed

Name	Title	Telephone	Cell	E-mail
	Security Coordinator			
	Alternate Security Coordinator			

Review Team

Name	Title	Location Assignment	Telephone	E-mail
	Lead	SSI		
	Secondary	SSI		
	TSS	TSA - HQ		

Supervisory Approval

Name	Title	Location Assignment	Telephone	E-mail
	STSI			
	AFSD-I			

TSA Headquarters Approval

Name	Title	Location Assignment	Telephone	E-mail
	Program Manager	HQ		
		HQ		

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Pipeline Corporate Security Review (CSR)	CSR FY2020 V.1 (October 2019)
Operator Name:	Assessment Date:
0	1/1/2019

Question Type	Question #	CSR Question	Answer (Yes/No/X)	
SAI	1.0000	Security Plans		
	1.0100	Is your corporate security manager solely dedicated to a corporate security function or tasked with other responsibilities such as environmental, health, and safety?		
	1.0200	Does your corporate security manager or equivalent position have a direct reporting relationship to the senior leadership in the corporation?		
	1.0300	Does the corporation have a cross-departmental security committee?		
	1.0400	Which of the following departments are represented on the security committee?	ZZZ	
	1.0401	Corporate Management		
	1.0402	Human Resources		
	1.0403	Security		
	1.0404	Legal		
	1.0405	Engineering		
	1.0406	Operations and/or Maintenance		
	1.0407	Information Technology		
	1.0408	Other (if checked, elaborate)		
R	1.0500	Have you established a corporate security program to address and document policies and procedures for managing security-related threats, incidents, and responses?		
R	1.0600	Does your corporation have a written corporate security plan?		
R	1.0700	Which of the following company plans are directly included or incorporated by reference in the corporate security plan?		
	1.0701	Business Continuity Plan		
	1.0702	Incident Response Plan		
	1.0703	Incident Recovery Plan		
	1.0704	Enterprise Cybersecurity Plans		
	1.0705	OT Cybersecurity Plans		
	1.0706	Other (if checked, elaborate)		
R	1.0800	Is the corporate security plan reviewed on an annual basis and updated as required?		
R	1.0900	Does the corporate security plan identify the primary and alternate security manager or officer responsible for executing and maintaining the plan?		
	1.1000	Is the corporate security plan readily available to those persons responsible for security actions?		
R	1.1100	Do you incorporate the following elements into your corporate security plan or associated documents?		

	1.1101	System Description		
	1.1102	Security Administration and Management Structure		
	1.1103	Risk Analysis and Assessments		
	1.1104	Physical Security and Access Control Measures		
	1.1105	Equipment Maintenance and Testing		
	1.1106	Personnel Screening		
	1.1107	Communications		
	1.1108	Personnel Training		
	1.1109	Security Incident Procedures		
	1.1110	National Terrorism Advisory System (NTAS) Response Procedures		
	1.1111	Security Plan Reviews		
	1.1112	Recordkeeping		
	1.1113	Cyber/SCADA System Security Measures		
	1.1114	Essential Security Contacts		
	1.1115	Security Testing and Audits		
	1.1116	Outreach (neighbors, law enforcement, media, public)		
	1.1117	Other (if checked, elaborate)		
R	1.1200	Do you have sufficient resources, including trained staff and equipment, to effectively execute the corporate security program?		
R	1.1300	Are appropriate financial resources allocated in the corporate budgeting and purchasing process to correct identified security deficiencies?		
	1.1400	How much operations and/or maintenance money did your corporation spend on security in the previous fiscal year?	ZZZ	
	1.1401	< $99,999		
	1.1402	$100,000 - $249,999		
	1.1403	$250,000 - $499,999		
	1.1404	$500,000 - $999,999		
	1.1405	$1,000,000 - $4,999,999		
	1.1406	>$5,000,000		
	1.1500	How much capital money did your corporation spend on security in the previous fiscal year?	ZZZ	
	1.1501	< $99,999		
	1.1502	$100,000 - $249,999		
	1.1503	$250,000 - $499,999		
	1.1504	$500,000 - $999,999		
	1.1505	$1,000,000 - $4,999,999		
	1.1506	>$5,000,000		
	1.1600	Has your corporation established security metrics?		
R	1.1700	Are the corporate security plan, the enterprise cyber security plan, and the OT cyber security plan, as applicable, protected from unauthorized access?		
R	1.1800	Are the corporate security plan, the enterprise cyber security plan, and the OT cyber security plan, as applicable, available for TSA review upon request?		
SAI	2.0000	**Security Plans - Cyber**		

	2.0100	Do your cybersecurity plans incorporate any of the following approaches?		
	2.0101	National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity		
	2.0102	U.S. Department of Energy, Office of Electricity and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance		
	2.0103	U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance		
	2.0104	Industry-specific methodologies (See 2018 TSA Pipeline Security Guidelines, Section 7.4 for partial listing.)		
	2.0105	Other (if checked, elaborate)		
R	2.0200	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?		
R	2.0300	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?		
R	2.0400	Has your corporation established policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams?		
R	2.0500	Has your corporation established and maintained a cyber-incident response capability?		
R	2.0600	For critical pipeline cyber assets, has your corporation established and maintained a process that supports 24/7 cyber-incident response?		
R	2.0700	Do your corporation's response plans and procedures include mitigation measures to help prevent further impacts?		
R	2.0800	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?		
R	2.0900	Does your corporation review its cyber recovery plan annually and update it as necessary?		
SAI	3.0000	Communication		
R	3.0100	Does your corporation have internal and external notification requirements and procedures for security events?		
R	3.0200	Does your corporation document and periodically update contact and communication information for Federal, state, and local homeland security/law enforcement agencies?		
R	3.0300	Does your corporation have a defined process for receiving, handling, disseminating, and storing security and threat information?		
R	3.0400	Do all critical facilities have primary and alternate communication capabilities for internal and external reporting of appropriate security events and information?		

	3.0500	Which of the following external agencies/organizations would the corporation notify in the event of a security incident, a security threat, or suspicious activity?	ZZZ	
	3.0501	National Response Center (NRC)		
	3.0502	Local emergency responders/911		
	3.0503	Transportation Security Administration / Transportation Security Operations Center (TSA/TSOC)		
	3.0504	Tribal emergency responders		
	3.0505	State emergency responders		
	3.0506	Other federal agencies		
	3.0507	Federal Bureau of Investigation (FBI)		
	3.0508	Department of Homeland Security (DHS)		
	3.0509	Neighboring corporations		
	3.0510	Other (if checked, elaborate)		
SAI	4.0000	Security Incident Procedures		
R	4.0100	Are security elements developed and maintained within the corporate incident response and recovery plan?		
	4.0200	Does your corporation have a policy and/or procedure for handling security threat or incident information?		
	4.0300	From whom does your corporation receive current security threat information?	ZZZ	
	4.0301	Transportation Security Operations Center (TSOC)		
	4.0302	DHS Protective Security Advisor (DHS PSA)		
	4.0303	Joint Terrorism Task Force (JTTF)		
	4.0304	Federal Bureau of Investigation (FBI)		
	4.0305	Homeland Security Information Network (HSIN)		
	4.0306	State fusion center(s)		
	4.0307	Local law enforcement		
	4.0308	Coast Guard		
	4.0309	Corporate affiliations		
	4.0310	Department of Energy		
	4.0311	Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)		
	4.0312	Other (if checked, elaborate)		
R	4.0400	Does your corporation notify TSA via the Transportation Security Operations Center (TSOC) by phone or email as soon as possible if any of the types of security incidents listed in Appendix B – TSA Notification Criteria, 2018 TSA Pipeline Security Guidelines occurs or if there is any other reason to believe that a terrorist incident may be planned or may have occurred?		
R	4.0500	Has your corporation implemented procedures for responding to security incidents or emergencies and to pertinent National Terrorism Advisory System (NTAS) Bulletins or Alerts, including appropriate reporting requirements?		
R	4.0600	Has your corporation implemented site-specific security measures for each critical facility to be taken in response to pertinent NTAS Bulletins or Alerts or other threat information?		

R	4.0700	Are the site-specific security measures for each critical facility reviewed and updated as necessary at least every 18 months?		
R	4.0800	Does your corporation have adequate staffing to implement security measures in response to security threat information?		
	4.0900	Does your corporation have contracts in place with private security providers to augment existing security staffing during times of heightened alert?		
R	4.1000	Are bomb threat checklists posted by telephones at all staffed facilities?		
R	4.1100	At an Elevated Threat Level, would your corporation enact the following physical access controls at your critical facilities?		
	4.1101	Limit facility access to essential personnel.		
	4.1102	Limit facility access to essential visitors, personnel, and vehicles.		
	4.1103	Increase surveillance of critical areas and facilities.		
	4.1104	Restrict deliveries to those essential to continued operations.		
	4.1105	Conduct random inspections of vehicles and of bags, backpacks, purses, etc.		
	4.1106	Delay or reschedule nonvital maintenance and capital project work that could affect facility security, as appropriate.		
	4.1107	Increase lighting in facility buffer zones, as appropriate.		
	4.1108	Verify the operating condition of security systems such as intrusion detection, cameras, and lighting initially and at least weekly thereafter until termination of the advisory.		
	4.1109	Request that local law enforcement agencies increase the frequency of patrols of the facility.		
	4.1110	Other (if checked, elaborate)		
R	4.1200	At an Elevated Threat Level, would your corporation enact the following measures on your cyber/SCADA system(s)?		
	4.1201	Increase monitoring of intrusion detection systems.		
	4.1202	Remind personnel of the reporting requirements for any unusual enterprise or control systems network activity.		
	4.1203	Remind personnel to be vigilant regarding suspicious electronic mail.		
	4.1204	Other (if checked, elaborate)		
R	4.1300	At an Elevated Threat Level, would your corporation enact the following communications measures at your critical facilities?		
	4.1301	Inform all employees and on-site contractors of the change to the Elevated Threat Level.		
	4.1302	Conduct security awareness briefings for all employees and on-site contractors.		
	4.1303	Brief employees and on-site contractors on the characteristics of suspicious packages or mail.		
	4.1304	Review response procedures for suspicious packages or mail.		
	4.1305	Inform local law enforcement that the facility is at an Elevated Threat Level and advise them of the security measures being employed.		

	4.1306	Verify the proper operation of intelligence and emergency communications networks/channels, including those with TSA and first responder agencies.		
	4.1307	Monitor these networks/channels as appropriate.		
	4.1308	Other (if checked, elaborate)		
R	4.1400	At an Imminent Threat Level, would your corporation enact the following physical access controls at your critical facilities?		
	4.1401	Cancel or delay non-vital contractor work and services.		
	4.1402	Allow deliveries by appointment only.		
	4.1403	Inspect all bags, backpacks, purses, etc. prior to entering the facility.		
	4.1404	Inspect all vehicles prior to gaining access to the facility.		
	4.1405	Inspect all deliveries, including packages and cargo.		
	4.1406	Secure all non-essential entrances and facility access points.		
	4.1407	Staff or monitor active facility entrances and access points 24/7.		
	4.1408	Erect barriers and/or obstacles to control vehicular traffic flow.		
	4.1409	Where possible, restrict vehicle parking to 150 feet from all critical areas and assets.		
	4.1410	Coordinate with local authorities regarding closing nearby public roads and facilities, if appropriate.		
	4.1411	Other (if checked, elaborate)		
R	4.1500	At an Imminent Threat Level, would your corporation enact the following measures on your cyber/SCADA system(s)?		
	4.1501	Limit network communications links to essential sites/users.		
	4.1502	Review remote access for individuals and revoke any credentials that are not current and necessary.		
	4.1503	Other (if checked, elaborate)		
R	4.1600	At an Imminent Threat Level, would your corporation enact the following communications measures?		
	4.1601	Inform all employees and contractors of the increase to the Imminent Threat Level.		
	4.1602	Conduct daily security and awareness briefings for each shift.		
	4.1603	Participate in situation update briefings with TSA, other government agencies including local law enforcement, and pipeline industry associations.		
	4.1604	Other (if checked, elaborate)		
	4.1700	Does your corporation use an incident management system, such as the National Incident Management System (NIMS), for security-related events?		
	4.1800	Does your company have a process for assuring the viability of the OT cyber recovery plan, including a backup control center?		
SAI	5.0000	Security Training		
R	5.0100	Does your corporation provide security awareness briefings, to include security incident recognition and reporting procedures, for all personnel with unescorted access upon hiring and every three years thereafter?		

R	5.0200	Does your corporation document security training and maintain records in accordance with company record retention policy?	
R	5.0300	Does your corporation provide security training, to include incident response training, to personnel assigned security duties upon hiring and annually thereafter?	
	5.0400	Have your corporation's security personnel availed themselves of any of the following training opportunities or affiliations?	
	5.0401	Security forums or conferences	
	5.0402	Pipeline forums or conferences	
	5.0403	Advanced security training	
	5.0404	Security Committee(s) participation	
	5.0405	Government Sector Committee(s)	
	5.0406	Industry security collaboration	
	5.0407	Other (if checked, elaborate)	
	5.0500	Does your corporation use any of the TSA security training material?	
R	5.0600	Do all persons requiring access to the company's pipeline cyber assets receive cybersecurity awareness training?	
R	5.0700	Is there a cyber-threat awareness program for employees that includes practical exercises/testing?	
R	5.0800	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?	
SAI	6.0000	Outreach	
R	6.0100	Does each critical facility conduct outreach to nearby law enforcement agencies to ensure awareness of the facility's functions and significance?	
R	6.0200	Does each critical facility conduct outreach to neighboring businesses to coordinate security efforts and to neighboring residences to provide facility security awareness?	
R	6.0300	For critical pipeline cyber assets, does your corporation ensure that threat and vulnerability information received from information-sharing forums and sources are made available to those responsible for assessing and determining the appropriate course of action?	
R	6.0400	Does your corporation report significant cyber incidents to the following?	
	6.0401	Senior management	
	6.0402	Appropriate federal entities	
	6.0403	Appropriate state, local, and tribal entities	
	6.0404	Applicable ISAC(s)	
R	6.0500	Does the corporation have procedures in place to contact the National Cybersecurity and Communications Integration Center (NCCIC) 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.)	

SAI	7.0000	Risk Analysis and Assessments		
R	7.0100	Does your corporation conduct criticality assessments for all facilities at least every 18 months?		
R	7.0200	Is the methodology used to determine critical facilities documented in the corporate security plan?		
R	7.0300	Did you utilize the criteria from the 2018 TSA Pipeline Security Guidelines to determine your list of critical facilities?		
R	7.0400	During the criticality assessment of your facilities, were all of the following criteria considered?		
	7.0401	Critical to national defense		
	7.0402	Key infrastructure		
	7.0403	Mass casualty or significant health effects		
	7.0404	Disruption to state or local government public or emergency services		
	7.0405	National landmarks or monuments		
	7.0406	Major rivers, lakes, or waterways		
	7.0407	Deliverability to significant number of customers		
	7.0408	Signifcantly disrupt pipeline system operations for an extended period of time, i.e., business critical facilities		
	7.0409	Other (if checked, elaborate)		
R	7.0500	Does your corporation conduct a security vulnerability assessment (SVA) or equivalent of each critical facility at least every 36 months?		
R	7.0600	Does your corporation conduct an SVA or equivalent within 12 months after achieving operational status for newly identified or constructed facilities?		
R	7.0700	Does your corporation conduct an SVA or equivalent of any critical facility within 12 months of completing a significant enhancement or modification to the facility?		
R	7.0800	Upon completion of an SVA or equivalent, are corrective actions implemented within 24 months?		
R	7.0900	Are assessment results documented and retained until no longer valid?		
	7.1000	Does your corporation conduct SVAs or equivalent on your non-critical facilities?		
R	7.1100	When conducting an SVA or equivalent, do you use one or more of the following methodologies?		
	7.1101	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER)		
	7.1102	American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA)		
	7.1103	Mission, Symbolism, History, Accessibility, Recognizability, Population, Proximity (MSHARPP)		
	7.1104	Third-party or corporate proprietary		
	7.1105	Other (if checked, elaborate)		
R	7.1200	Does your corporation integrate security risk mitigation measures during the design, construction, or renovation of a facility?		
SAI	8.0000	Risk Analysis and Assessments - Cyber		

R	8.0100	Does your corporation evaluate and classify pipeline cyber assets using the following criteria?		
	8.0101	Critical pipeline cyber assets are operational technologies (OT) systems that can control operations on the pipeline.		
	8.0102	Non-critical pipeline cyber assets are OT systems that monitor operations on the pipeline.		
R	8.0200	Does your corporation review and assess pipeline cyber asset classification as critical or noncritical at least every 12 months?		
R	8.0300	Has your corporation established and distributed cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment?		
R	8.0400	Has your corporation established a process to identify and evaluate vulnerabilities and compensating security controls?		
	8.0500	Does the process address unmitigated/accepted vulnerabilities in the OT environment?		
R	8.0600	Does your corporation conduct cyber vulnerability assessments as described in your risk assessment process?		
R	8.0700	For critical pipeline cyber assets, does your corporation use independent assessors to conduct pipeline cybersecurity assessments?		
SAI	9.0000	**Drills & Exercises**		
R	9.0100	Does your corporation conduct periodic security drills and exercises for all facilities, including in conjunction with other required drills or exercises?		
R	9.0200	Does your corporation require each critical facility to conduct or participate in an annual security drill or exercise, including common drills or exercises in which multiple facilities may participate?		
R	9.0300	Does your corporation require each critical facility to prepare a written post-event report assessing security drills and exercises and documenting corrective actions?		
	9.0400	Over the past three years, with whom has your corporation participated in security drills or exercises?	ZZZ	
	9.0401	Local emergency responders		
	9.0402	Tribal emergency responders		
	9.0403	State emergency responders		
	9.0404	Federal emergency responders		
	9.0405	Federal Bureau of Investigation (FBI)		
	9.0406	Department of Homeland Security (DHS)		
	9.0407	Transportation Security Administration (TSA)		
	9.0408	Neighboring corporations		
	9.0409	Other (if checked, elaborate)		
R	9.0500	Does the corporate security plan include policies and procedures for auditing and testing the effectiveness of the company's security procedures, to include documentation of results?		
R	9.0600	For critical pipeline cyber assets, are cybersecurity incident response exercises conducted periodically?		

SAI	10.0000	Cyber Security		
R	10.0100	Has your corporation established and documented policies and procedures for the following?		
	10.0101	Assessing and maintaining configuration information.		
	10.0102	Tracking changes made to pipeline cyber assets.		
	10.0103	Patching/upgrading operating systems and applications.		
	10.0104	Ensuring that the changes do not adversely impact existing cybersecurity controls.		
	10.0105	Other (if checked, elaborate)		
R	10.0200	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?		
	10.0300	For critical pipeline cyber assets, is there a defined list of software programs authorized to execute in the operating system?		
R	10.0400	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?		
	10.0500	Are methods in place to verify the accuracy of the diagrams and/or other documentation related to your OT system?		
R	10.0600	For critical pipeline cyber assets, does your corporation employ mechanisms to detect unauthorized components?		
R	10.0700	For critical pipeline cyber assets, does your corporation review network connections periodically, including remote access and third-party connections?		
R	10.0800	For critical pipeline cyber assets, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints?		
R	10.0900	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 measuresbeing applied?		
R	10.1000	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?		
R	10.1100	Has your corporation implemented the following measures?		
	10.1101	Establish and enforce unique accounts for each individual user and administrator.		
	10.1102	Establish security requirements for certain types of privileged accounts.		
	10.1103	Prohibit the sharing of these accounts.		
	10.1200	Are authentication methods and specific standards employed throughout your company's cyber access control environment?		
R	10.1300	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?		
R	10.1400	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?		

R	10.1500	Has your corporation implemented the following measures?		
	10.1501	Establish and enforce access control policies for local and remote users.		
	10.1502	Have procedures and controls in place for approving and enforcing remote and third-party connections.		
R	10.1600	Does your corporation ensure appropriate segregation of duties is in place and, where this is not feasible, apply appropriate compensating security controls?		
R	10.1700	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)?		
R	10.1800	For critical pipeline cyber assets, has your corporation implemented the following measures?		
	10.1801	Restrict user physical access to control systems and control networks by using appropriate controls.		
	10.1802	Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).		
R	10.1900	Does your corporation monitor physical and remote user access to critical pipeline cyber assets?		
R	10.2000	Does your corporation employ mechanisms (e.g., active directory) to support the management of accounts for critical pipeline cyber assets?		
R	10.2100	Has your corporation established and implemented policies and procedures to ensure data protection measures are in place, including the following?		
	10.2101	Identifying critical data and establishing classification of different types of data.		
	10.2102	Establishing specific data handling procedures.		
	10.2103	Establishing specific data disposal procedures.		
	10.2200	If data protection measures are not in place, are compensating controls in place?		
R	10.2300	Are pipeline cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections?		
	10.2400	Does the OT system deny network traffic by default and allow only authorized network traffic?		
	10.2500	Does the OT system monitor and manage communications at appropriate OT network boundaries?		
	10.2600	Do OT system controls protect the integrity of electronically-communicated information? (e.g., preventing man in the middle)?		
	10.2700	Does the OT system prevent traffic from being routed to the internet?		
R	10.2800	Does your corporation regularly validate that technical controls comply with the company's cybersecurity policies, plans, and procedures, and report results to senior management?		
R	10.2900	Has your corporation implemented technical or procedural controls to restrict the use of pipeline cyber assets to only approved activities?		

R	10.3000	Has your corporation implemented processes to respond to anomalous activity through the following?		
	10.3001	Generating alerts and responding to them in a timely manner.		
	10.3002	Logging cybersecurity events and reviewing these logs.		
R	10.3100	Does your corporation monitor for unauthorized access or the introduction of malicious code or communications?		
R	10.3200	Has your corporation established technical or procedural controls for cyber intrusion monitoring and detection?		
R	10.3300	Does your corporation perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?		
SAI	11.0000	Physical Security & Access Control		
	11.0100	Which of the following security measures does your corporate security plan require at critical facilities?	ZZZ	
	11.0101	Fences		
	11.0102	Gates equivalent to attached barriers		
	11.0103	Signage such as No Trespassing, Do Not Enter, Authorized Personnel Only, CCTV in Use, etc.		
	11.0104	Closed circuit television (CCTV)		
	11.0105	Intrusion sensors		
	11.0106	Alarms		
	11.0107	Clear zones around fence lines		
	11.0108	Locks		
	11.0109	Barriers such as bollards, planters, or Jersey barriers		
	11.0110	Tamper devices		
	11.0111	Patrols		
	11.0112	Lighting		
	11.0113	Crime Prevention Through Environmental Design (CPTED)		
	11.0114	Unarmed Guards		
	11.0115	Armed Guards		
	11.0116	Video-analytic Systems		
	11.0117	Video Recording		
	11.0118	Intrustion-detection Systems		
	11.0119	Other (if checked, elaborate)		
	11.0200	How does your corporation physically control access to controlled-access areas?	ZZZ	
	11.0201	Lock and Key		
	11.0202	Biometric reader		
	11.0203	Digital keycard		
	11.0204	PIN Code		
	11.0205	Proximity Card		
	11.0206	Radio Remote Control		
	11.0207	Other (if checked, elaborate)		
	11.0300	Which of the following security measures does your corporate security plan require at all facilities?	ZZZ	

	11.0301	Fences		
	11.0302	Gates equivalent to attached barriers		
	11.0303	Signage such as No Trespassing, Do Not Enter, Authorized Personnel Only, CCTV in Use, etc.		
	11.0304	Closed circuit television (CCTV)		
	11.0305	Intrusion sensors		
	11.0306	Alarms		
	11.0307	Clear zones around fence lines		
	11.0308	Locks		
	11.0309	Barriers such as bollards, planters, or Jersey barriers		
	11.0310	Tamper devices		
	11.0311	Patrols		
	11.0312	Lighting		
	11.0313	Crime Prevention Through Environmental Design (CPTED)		
	11.0314	Unarmed Guards		
	11.0315	Armed Guards		
	11.0316	Video-analytic Systems		
	11.0317	Video Recording		
	11.0318	Intrustion-detection Systems		
	11.0319	Other (if checked, elaborate)		
R	11.0400	Does the corporate security plan require the following security measures at all facilities?		
	11.0401	Employ measures to impede unauthorized persons from gaining access to a facility and restricted areas within a facility.		
	11.0402	Close and secure perimeter gates or entrances when not in use.		
	11.0403	Post "No Trespassing" or "Authorized Personnel Only" signs at intervals that are visible from any point of potential entry.		
R	11.0500	Does the corporate security plan require the following security measures at all facilities?		
	11.0501	Employ measures to impede unauthorized access to facilities.		
	11.0502	Maintain fences, if used, without gaps around gates or underneath the fence line.		
	11.0503	Ensure that there is a clear zone for several feet on either side of the fence, free of obstructions, vegetation, or objects that could be used for concealment or to scale the fence.		
R	11.0600	Does the corporate security plan require that each critical facility implement procedures (e.g., manual or electronic sign in/out) for controlling access to the facility and restricted buildings or areas within the facility?		
R	11.0700	Does the corporate security plan require that each critical facility create a security perimeter that impedes unauthorized vehicles from entering the facility perimeter or critical areas by installing and maintaining barriers (e.g., fences, bollards, jersey barriers)?		

R	11.0800	Does the corporate security plan require that each critical facility ensure that visitors are monitored and escorted?		
R	11.0900	Does the corporate security plan require that each critical facility install and maintain gates of an equivalent quality to the barrier to which they are attached?		
R	11.1000	Does the corporate security plan require that each critical facility provide sufficient illumination for human and technological recognition of intrusion into the facility perimeter or critical areas?		
R	11.1100	Does the corporate security plan require that each critical facility or critical areas within a facility have security measures to monitor, detect, and assess 24 hours per day, 7 days per week?		
R	11.1200	Does your corporation have key control procedures for key issuance, tracking, collection, loss, and unauthorized duplication?		
R	11.1300	Does your corporation conduct a key inventory at least every 24 months?		
R	11.1400	Does your corporation use patent keys to prevent unauthorized duplication?		
SAI	12.0000	Personnel Security		
R	12.0100	Has your corporation established policies and procedures for applicant pre-employment screening and behavioral criteria for disqualification of applicants and employees?		
	12.0200	Is there at least one individual within your corporation who holds a current federal security clearance?		
	12.0300	What is the highest level of clearance that is held within your corporation?	ZZZ	
	12.0301	Secret		
	12.0302	Top Secret		
	12.0303	Top Secret SCI		
	12.0400	Does your corporation conduct pre-employment background investigations on all potential employees?		
R	12.0500	Does your corporation conduct pre-employment background investigations of applicants for positions that involve any of the following?		
	12.0501	Authorized regular unescorted access to control systems or sensitive areas.		
	12.0502	Authorized access to sensitive information.		
	12.0503	Assigned security roles		
	12.0504	Assigned to work at or granted access rights to critical facilities.		
	12.0600	Does your corporation have a designated individual solely responsible for cyber/SCADA security?		
R	12.0700	Do pre-employment background investigations of applicants for positions described in Question 12.0500 above include all of the following?		
	12.0701	Verification and validation of identity		
	12.0702	Criminal history check		
	12.0703	Verification and validation of legal authorization to work		

R	12.0800	Has your corporation developed identification and badging policies and procedures for personnel who have access to secure areas or sensitive information that address the following?		
	12.0801	Lost or stolen identification cards or badges		
	12.0802	Temporary badges		
	12.0803	Personnel termination		
	12.0900	Does your corporation use the federally-established list of disqualifying crimes (listed in 49 CFR 1572.103) to assess the suitability of personnel for positions described in Question 12.0500 above?		
R	12.1000	Does your corporation conduct recurring background investigations at least every ten years for employees occupying security positions or who have access to sensitive information or areas?		
R	12.1100	Does the corporate security plan require that each critical facility ensure that company or vendor identification is available for examination by being visibly displayed or carried by personnel while on-site?		
R	12.1200	Does your corporation verify that contractors have background investigation policies and procedures at least as rigorous as the corporation's?		
R	12.1300	Does the corporate security plan require that each critical facility ensure personnel identification cards or badges are secure from tampering and contain the individual's photograph and name?		
	12.1400	Does your corporation have a policy and/or procedure in place addressing security issues related to employee termination?		
	12.1500	Are the following actions taken during termination activities?		
	12.1501	Retrieve badge or identification card.		
	12.1502	Disable passwords.		
	12.1503	Retrieve keys.		
	12.1504	Retrieve operational and/or security manuals.		
	12.1505	Block computer-system access.		
	12.1506	Discharged employee signs nondisclosure agreement.		
	12.1507	Other (if checked, elaborate)		
SAI	13.0000	**Equipment Maintenance and Testing**		
R	13.0100	Has your corporation implemented a maintenance program to ensure that security systems are in good working order?		
R	13.0200	Does your corporation identify and respond to security equipment malfunctions or failures in a timely manner?		
R	13.0300	Do all critical facilities, through routine use or quarterly examination, verify the proper operation and/or condition of all security equipment?		
R	13.0400	Do all critical facilities provide an equivalent level of protective security measures to mitigate risk during power outages, security equipment failure, or extended repair of security systems?		
	13.0500	Does your corporate security maintenance program include all of the following?		
	13.0501	Corrective maintenance		
	13.0502	Preventive maintenance		

	13.0503	Testing		
	13.0504	Inspection		
SAI	**14.0000**	**Recordkeeping**		
R	14.0100	Does the corporate security plan address recordkeeping policies and procedures for security information, including the protection of Sensitive Security Information (SSI) in accordance with the provisions of 49 CFR Parts 15 and 1520?		
R	14.0200	Do all facilities retain the following documents, as appropriate, until superseded or replaced?		
	14.0201	Corporate security plan		
	14.0202	Criticality assessment(s)		
	14.0203	Training records		
	14.0204	Security drill or exercise reports		
	14.0205	Incident response plan(s)		
	14.0206	Security testing and audits		
R	14.0300	In addition to the documents listed in Question 14.0200 above, does each critical facility retain the following documents until superseded or replaced?		
	14.0301	SVA(s)		
	14.0302	Site-specific security measures		
	14.0400	Does your corporation have a document-marking policy or procedure?		
R	14.0500	Does the corporation make the security information records described in Questions 14.0200 and 14.0300 above available to TSA upon request?		
	14.0600	Has your corporation taken any of the following steps to apply operations security (OPSEC) in daily activities?		
	14.0601	Mark documents.		
	14.0602	Hold conversations in appropriate locations.		
	14.0603	Report undue interest in pipeline security or operations.		
	14.0604	Secure sensitive documents outside of office areas such as in vehicles or in transport.		
	14.0605	Dispose of documents properly.		
	14.0606	Dispose of computer equipment and associated media securely.		
	14.0607	Create strong passwords.		
	14.0608	Change passwords periodically.		
	14.0609	Vary patterns of behavior		
	14.0610	Remove badges in public		
	14.0611	Other (if checked, elaborate)		
R	14.0700	Does your corporation maintain and secure criticality assessments, critical facility lists, and security vulnerability assessments or equivalent?		

		DEPARTMENT OF HOMELAND SECURITY		
		Transportation Security Administration		
		Pipeline Corporate Security Review (CSR) IT Questions	**CSR FY2020 V.1 (October 2019)**	
		Operator Name:	Assessment Date:	
		0	1/1/2019	

Question Type	Question #	CSR Question	Answer (Yes/No/X)	
SAI	**2.0000**	**Security Plans - Cyber**		
	2.0100	Do your cybersecurity plans incorporate any of the following approaches?		
	2.0101	National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity		
	2.0102	U.S. Department of Energy, Office of Electricity and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance		
	2.0103	U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance		
	2.0104	Industry-specific methodologies (See 2018 TSA Pipeline Security Guidelines, Section 7.4 for partial listing.)		
	2.0105	Other (if checked, elaborate)		
R	2.0200	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?		
R	2.0300	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?		
R	2.0400	Has your corporation established policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams?		
R	2.0500	Has your corporation established and maintained a cyber-incident response capability?		
R	2.0600	For critical pipeline cyber assets, has your corporation established and maintained a process that supports 24/7 cyber-incident response?		
R	2.0700	Do your corporation's response plans and procedures include mitigation measures to help prevent further impacts?		
R	2.0800	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?		
R	2.0900	Does your corporation review its cyber recovery plan annually and update it as necessary?		
SAI	**8.0000**	**Risk Analysis and Assessments - Cyber**		
R	8.0100	Does your corporation evaluate and classify pipeline cyber assets using the following criteria?		
	8.0101	Critical pipeline cyber assets are operational technologies (OT) systems that can control operations on the pipeline.		
	8.0102	Non-critical pipeline cyber assets are OT systems that monitor operations on the pipeline.		

R	8.0200	Does your corporation review and assess pipeline cyber asset classification as critical or noncritical at least every 12 months?		
R	8.0300	Has your corporation established and distributed cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment?		
R	8.0400	Has your corporation established a process to identify and evaluate vulnerabilities and compensating security controls?		
	8.0500	Does the process address unmitigated/accepted vulnerabilities in the OT environment?		
R	8.0600	Does your corporation conduct cyber vulnerability assessments as described in your risk assessment process?		
R	8.0700	For critical pipeline cyber assets, does your corporation use independent assessors to conduct pipeline cybersecurity assessments?		
SAI	10.0000	Cyber Security		
R	10.0100	Has your corporation established and documented policies and procedures for the following?		
	10.0101	Assessing and maintaining configuration information.		
	10.0102	Tracking changes made to pipeline cyber assets.		
	10.0103	Patching/upgrading operating systems and applications.		
	10.0104	Ensuring that the changes do not adversely impact existing cybersecurity controls.		
	10.0105	Other (if checked, elaborate)		
R	10.0200	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?		
	10.0300	For critical pipeline cyber assets, is there a defined list of software programs authorized to execute in the operating system?		
R	10.0400	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?		
	10.0500	Are methods in place to verify the accuracy of the diagrams and/or other documentation related to your OT system?		
R	10.0600	For critical pipeline cyber assets, does your corporation employ mechanisms to detect unauthorized components?		
R	10.0700	For critical pipeline cyber assets, does your corporation review network connections periodically, including remote access and third-party connections?		
R	10.0800	For critical pipeline cyber assets, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints?		
R	10.0900	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 measuresbeing applied?		
R	10.1000	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?		
R	10.1100	Has your corporation implemented the following measures?		
	10.1101	Establish and enforce unique accounts for each individual user and administrator.		

	10.1102	Establish security requirements for certain types of privileged accounts.		
	10.1103	Prohibit the sharing of these accounts.		
	10.1200	Are authentication methods and specific standards employed throughout your company's cyber access control environment?		
R	10.1300	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?		
R	10.1400	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?		
R	10.1500	Has your corporation implemented the following measures?		
	10.1501	Establish and enforce access control policies for local and remote users.		
	10.1502	Have procedures and controls in place for approving and enforcing remote and third-party connections.		
R	10.1600	Does your corporation ensure appropriate segregation of duties is in place and, where this is not feasible, apply appropriate compensating security controls?		
R	10.1700	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)?		
R	10.1800	For critical pipeline cyber assets, has your corporation implemented the following measures?		
	10.1801	Restrict user physical access to control systems and control networks by using appropriate controls.		
	10.1802	Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).		
R	10.1900	Does your corporation monitor physical and remote user access to critical pipeline cyber assets?		
R	10.2000	Does your corporation employ mechanisms (e.g., active directory) to support the management of accounts for critical pipeline cyber assets?		
R	10.2100	Has your corporation established and implemented policies and procedures to ensure data protection measures are in place, including the following?		
	10.2101	Identifying critical data and establishing classification of different types of data.		
	10.2102	Establishing specific data handling procedures.		
	10.2103	Establishing specific data disposal procedures.		
	10.2200	If data protection measures are not in place, are compensating controls in place?		
R	10.2300	Are pipeline cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections?		
	10.2400	Does the OT system deny network traffic by default and allow only authorized network traffic?		
	10.2500	Does the OT system monitor and manage communications at appropriate OT network boundaries?		
	10.2600	Do OT system controls protect the integrity of electronically-communicated information? (e.g., preventing man in the middle)?		

	10.2700	Does the OT system prevent traffic from being routed to the internet?		
R	10.2800	Does your corporation regularly validate that technical controls comply with the company's cybersecurity policies, plans, and procedures, and report results to senior management?		
R	10.2900	Has your corporation implemented technical or procedural controls to restrict the use of pipeline cyber assets to only approved activities?		
R	10.3000	Has your corporation implemented processes to respond to anomalous activity through the following?		
	10.3001	Generating alerts and responding to them in a timely manner.		
	10.3002	Logging cybersecurity events and reviewing these logs.		
R	10.3100	Does your corporation monitor for unauthorized access or the introduction of malicious code or communications?		
R	10.3200	Has your corporation established technical or procedural controls for cyber intrusion monitoring and detection?		
R	10.3300	Does your corporation perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?		

DEPARTMENT OF HOMELAND SECURITY			
Transportation Security Administration			
Pipeline Operator Overview		**CSR FY2020 V.1 (October 2019)**	
Operator Name		**Lead Inspector:**	0
0		**Assessment Date:**	1/1/2019

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION	Implementation	R Only	# of Recommendations
1	Security Plans	0%	0%	0
2	Security Plans - Cyber	0%	0%	0
3	Communication	0%	0%	0
4	Security Incident Procedures	0%	0%	0
5	Security Training	0%	0%	0
6	Outreach	0%	0%	0
7	Risk Analysis and Assessments	0%	0%	0
8	Risk Analysis and Assessments - Cyber	0%	0%	0
9	Drills & Exercises	0%	0%	0
10	Cyber Security	0%	0%	0
11	Physical Security & Access Control	0%	0%	0
12	Personnel Security	0%	0%	0
13	Equipment Maintenance and Testing	0%	0%	0
14	Recordkeeping	0%	0%	0
	Overall Implementation:	0.00%	0%	0

Color Key:

Requirements have been met.
Requirements are partially met and/or are in the process of being completed.
Does not meet requirements as described in reference materials.

0														
Current CSR vs. Previous CSR Comparison (R Only)														
	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	Overall
Current Operator CSR Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Previous Operator CSR Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Difference	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Implementation by SAI
Current Operator CSR Implementation vs. Previous CSR Implementation
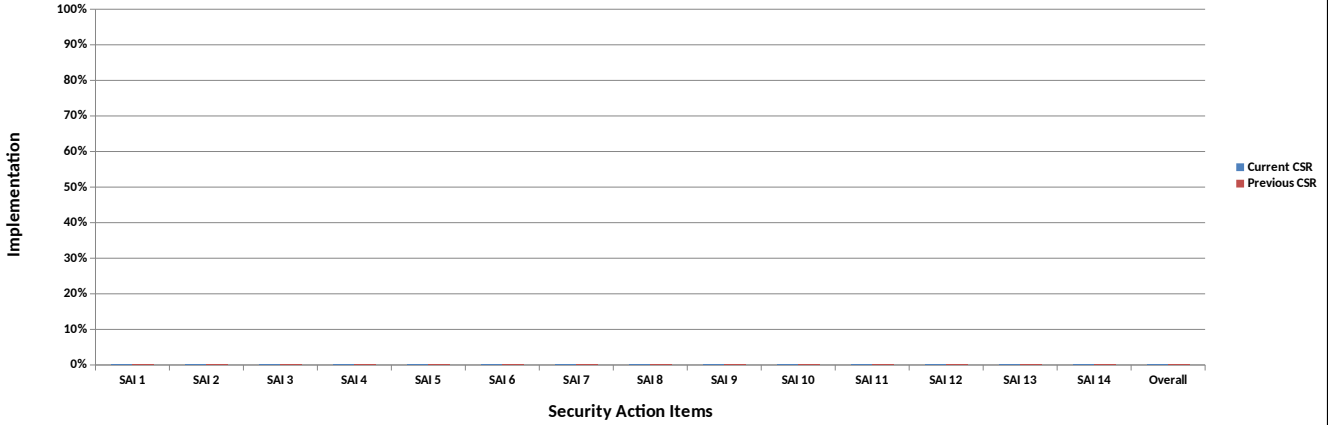
0														
Current CSR Recommendations vs. Previous CSR Recommendations Comparison														
	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	Total
Current Operator CSR Recommendations	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Previous Operator CSR Recommendations	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Difference	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Recommendations by SAI
Current Operator CSR Implementation vs. Previous CSR Implementation
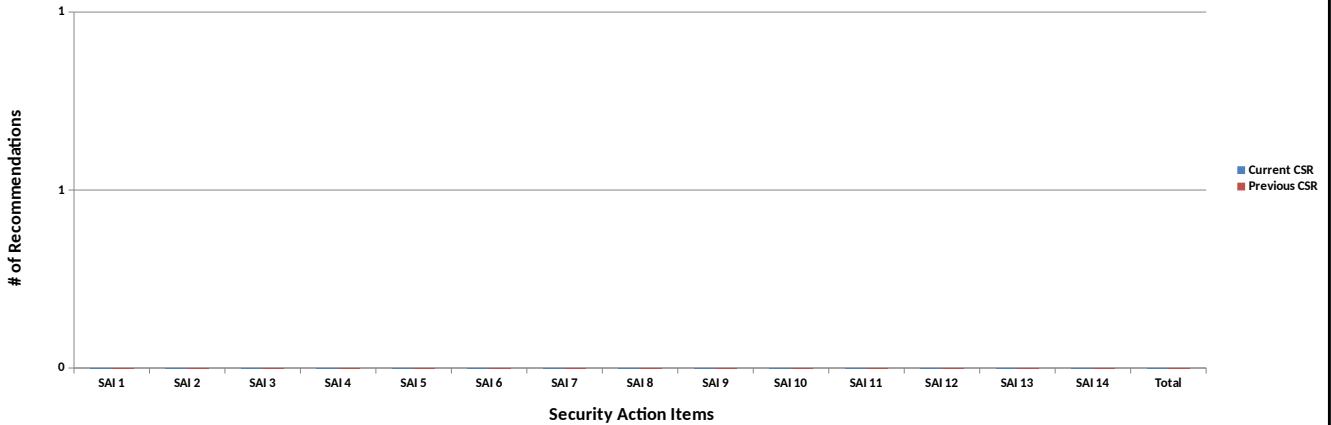
	0		
	Recommendations		

Recommendation #	CSR Question #	SAI Category	Recommendation Narrative
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			

38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			
62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			
73			
74			
75			
76			
77			
78			
79			
80			
81			
82			

83			
84			
85			
86			
87			
88			
89			
90			
91			
92			
93			
94			
95			
96			
97			
98			
99			
100			

CSR Recommendations Follow-up				
Pipeline Operator	**0**		**CSR Date:**	**1/1/2019**
Follow-up Request Date	**Stakeholder Response Date**		**18-24 Month Follow-up Window**	
			From:	To:
			7/1/2020	12/31/2020

Recommendation #	CSR Question #	Recommendation	Stakeholder Response Code
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			
62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			

Response Codes
1 - Recommendation has been completed/implemented
2 - Recommendation will be completed/implemented
3 - Recommendation being evaluated
4 - Recommendation will not be completed/implemented
5 - Recommendation no longer applicable

73			
74			
75			
76			
77			
78			
79			
80			
81			
82			
83			
84			
85			
86			
87			
88			
89			
90			
91			
92			
93			
94			
95			
96			
97			
98			
99			
100			

0			
Considerations			
Consideration #	CSR Question #	SAI Category	Consideration Narrative
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

		0			
Best Practices					
#	CSR Question #	SAI Category	Best Practice Description		
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

	0						
	Critical Facility List						
#	**Critical Facility Name**	**Address**	**City**	**State**	**Latitude**	**Longitude**	**Description / Notes**
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

SENSITIVE SECURITY INFORMATION

0
Meeting Attendees

	Date:	1/1/2019

TSA Pipeline Security Attendees					
Name	**Title**	**Division**	**Name**	**Title**	**Division**

Pipeline Corporation Attendees					
Name	**Title**	**Division**	**Name**	**Title**	**Division**

Other Attendees					
Name	**Title**	**Organization / Company**	**Name**	**Title**	**Organization / Company**

CSR Form Filled Out By					
Name	**Title**	**Division**	**Name**	**Title**	**Division**

SAI #	SAI Description
1	Security Plans
2	Security Plans - Cyber
3	Communication
4	Security Incident Procedures
5	Security Training
6	Outreach
7	Risk Analysis and Assessments
8	Risk Analysis and Assessments - Cyber
9	Drills & Exercises
10	Cyber Security
11	Physical Security & Access Control
12	Personnel Security
13	Equipment Maintenance and Testing
14	Recordkeeping

Paperwork Reduction Act Burden Statement: This is a voluntary collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 8 hours and an additional 3 hours for follow-up on TSA recommendations. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-0056, which expires on 02/29/2020. Send comments regarding this burden estimate or collection to: TSA-11, Attention: PRA 1652-0056 Pipeline CSR, 6565 Springfield Center Drive, Springfield, VA 22150.