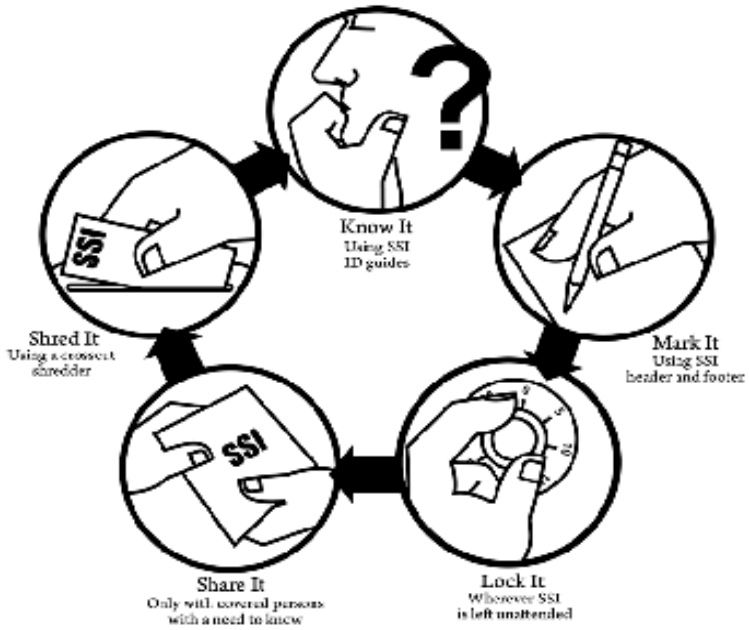
DEPARTMENT OF HOMELAND SECURITY

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

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

Pipeline Critical Facility Security Review (CFSR)

CFSR FY2022 V.1 PRA Draft (February 2021)

Transportation Security Administration

Date of Visit	TSA Field Office	Region #
2/26/2021	N/A (SSI - Contractor)	
Report Date	**HTUA Name**	
	<Please Select>	

TYPE OF VISIT	
Critical Facility Security Review	
Is This A Revisit?	**Date of Previous CFSR Interview/Visit?**
Is This A Virtual CFSR?	

Products Carried (mark applicable with "X"):			
	< Natural Gas/LNG		< Crude Oil
	< Refined Products		< NGL/LPG
	< Toxic Inhalation Hazard (TIH)		
	< Chemicals (list below)		
List >			

Name of Company/System/Facility					
Pipeline Company					
Pipeline System					
Pipeline Facility Name					
Facility Address					
City		**State**		**Zip Code**	
County					
Latitude (N)					
Longitude (W)					

Downstream Facilities - Select All That Apply and Describe

	Airport (CAT X)	
	Military Base	
	Power Generation Plant	
	Other Facility	

Primary Facility Function(s) - Select All That Apply

	Gas Compressor Station		Back-up Pipeline Control Center
	Liquids Pump Station		Marketing Terminal
	Natural Gas City Gate/Town Border Station		Underground Storage Capacity (note capacity)
	Pipeline Interconnect	>>>	Capacity:
	Meter/Regulator Station		Above Ground Storage Tanks (note capacity)
	Mainline Valve Site	>>>	Capacity:
	Bridge Span		LNG Peak Shaving Facility
	NGL/LPG Terminal		Toxic Inhalation Hazard (TIH) Facility
	Security Operations Center		Other (describe)
	Pipeline Control Center	>>>	Description:
	Inbound Pipeline (number, diameter, etc.)		Gas Volumes (describe)
>>>	Description:	>>>	Description:
	Outbound Pipeline (number, diameter, etc.)		Liquid Volumes (describe)
>>>	Description:	>>>	Description:
	Property (acreage inside perimeter fencing)		
>>>	Description:		

Note General Operational Characteristic
Include number of In-bound and Out-bound lines, pipe diameter, acreage, throughput (annual, daily monthly etc.)

Comments:

Describe the Most Significant Impact on Downstream/Upstream Customers if Facility Inoperable

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

Critical Facility Security Review (CFSR)

CFSR FY2022 V.1 PRA Draft (February 2021)

Pipeline Facility Name	Assessment Date:
0	2/26/2021

Question Type	Question #	CFSR Question	Answer Key	N/A (Select X)	Responses	Comments
SAI	0.0000	General Facility Information				
	0.0100	Is the facility staffed?	A - No C - Yes			
	0.0200	Staffing Periods?	A - 24/7 B - 7 days/week (days only) C - Monday-Friday, days and nights D - Monday-Friday, days only E - Monday-Friday, partial G - Other (describe) H - Varies with season I - Unknown			
	0.0300	Total number of personnel who are present at the critical facility during day shifts?	A - 0 B - 1-5 C - 6-15 D - 16-25 E - 26-35 F - 36+ H - Unknown			
	0.0400	Total number of personnel who are present at the critical facility during night/weekend/holiday shifts?	A - 0 B - 1-5 C - 6-15 D - 16-25 E - 26-35 F - 36+ H - Unknown			
	0.0500	Is the facility a shared site with another pipeline operator, utility, or commercial entity?	A - No B - Unknown C - Yes			
	0.0600	Is the facility located within the perimeter of another company's or operator's facility?	A - No B - Unknown C - Yes			
	0.0700	Is the facility located within the secured perimeter of a military base?	A - No B - Unknown C - Yes			

	0.0800	Is the facility regulated by the Maritime Transportation Security Act (MTSA)?	A - No B - Unknown C - Yes			
	0.0900	Is all or part of the facility regulated by the Chemical Facility Anti-Terrorism Standards (CFATS)?	A - No B - Unknown C - Yes			
SAI	**1.0000**	**Security Plans**				
	1.0001	There are no CFSR questions related to this SAI.	N/A		**N/A**	
SAI	**2.0000**	**Security Plans - Cyber**				
	2.0001	There are no CFSR questions related to this SAI.	N/A		**N/A**	
SAI	**3.0000**	**Communication**				
R	3.0100	Does the facility document and periodically update contact and communication information for Federal, state, and local homeland security/law enforcement agencies?	A - No B - Unknown C - Yes			
R	3.0200	Has the operator established a defined process for receiving, handling, disseminating, and storing security and threat information?	A - No B - Unknown C - Yes			
R	3.0300	Does the facility ensure primary and alternate communication capabilities exist for internal and external reporting of all appropriate security events and information?	A - No B - Unknown C - Yes			
SAI	**4.0000**	**Security Incident Procedures**				
R	4.0100	Has the facility implemented site-specific security measures to be taken in response to pertinent NTAS Bulletins or Alerts or other threat information?	A - No B - Unknown C - Yes			
R	4.0200	Are site-specific security measures and procedures reviewed and updated as necessary on a periodic basis not to exceed 18 months?	A - No B - Unknown C - Yes			
	4.0300	Has the facility received or identified any breach of security, or suspicious behavior in or around the facility during the past five years to include; bomb threats, suspicious photography and or surveillance. See Appendix B in the guidelines for additional examples.	A - No B - Unknown C - Yes			
R	4.0400	If yes to Question 4.0300, was Transportation Security Operations Center (TSOC) notified?	A - No B - Unknown C - Yes			
	4.0500	Note names of nearby law enforcement agencies (LEA).	[redacted]			
R	4.0600	Are bomb threat response checklists printed and readily accessible near facility telephones at staffed facilities?	A - No B - Unknown C - Yes			
SAI	**5.0000**	**Security Training**				

R	5.0100	Do facility personnel with unescorted access receive initial security awareness briefings, to include security incident recognition and reporting procedures upon hire?	A - No B - Unknown C - Yes			
R	5.0200	Are facility personnel with unescorted access required to complete security awareness briefings to include security incident recognition and reporting procedures training every three years or more frequently?	A - No B - Unknown C - Yes			
R	5.0300	Do facility personnel who are assigned, or are responsible for security duties receive initial security training (including incident response training) upon hire and annually thereafter?	A - No B - Unknown C - Yes			
	5.0400	Does the security awareness training include information from TSA developed training materials?	A - No B - Unknown C - Yes			
R	5.0500	Does the operator document and maintain security training records in accordance with company record retention policy?	A - No B - Unknown C - Yes			
R	5.0600	Do all persons requiring access to the company's pipeline cyber assets (e.g. SCADA, PCS and DCS) receive cybersecurity awareness training?	A - No B - Unknown C - Yes			
R	5.0700	Do operators receive role-based security training on recognizing and reporting potential indicators of system compromise prior to granting them access to the facility's SCADA system or equivalent OT system?	A - No B - Unknown C - Yes			
SAI	**6.0000**	**Outreach**				
R	6.0100	Has the facility conducted outreach to nearby law enforcement agencies to ensure awareness of the facility's functions and significance?	A - No B - Unknown C - Yes			
	6.0200	Question Removed. Space Reserved for Future Use.		X		Question Removed. Space Reserved for Future Use.
R	6.0300	Does the operator conduct outreach to neighboring businesses (e.g.. pipeline facilities and refineries) to coordinate security efforts, and to neighboring residences to provide facility security awareness? (e.g.. See something say something)	A - No B - Unknown C - Yes			
	6.0400	Which type of security outreach efforts apply? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	6.0401	Public security awareness mailings				
	6.0402	Operator's corporate web site				
	6.0403	Local public meetings				
	6.0404	Direct contact at residences and commercial facilities				
	6.0405	N/A				
	6.0406	Other (describe)				
SAI	**7.0000**	**Risk Analysis and Assessments**				

	7.0100	Based on the criteria presented in the TSA Pipeline Security Guidelines, why is the facility designated "critical?" Select all that apply.	Select With "X" In Green Cells		ZZZ	
	7.0101	Criterion 1				
	7.0102	Criterion 2				
	7.0103	Criterion 3				
	7.0104	Criterion 4				
	7.0105	Criterion 5				
	7.0106	Criterion 6				
	7.0107	Criterion 7				
	7.0108	Criterion 8				
	7.0109	Other (describe)				
	7.0200	Which components are most vital to the facility's continued operations? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	7.0201	Electrical power infrastructure (substation, switchgear, etc.)				
	7.0202	Computer/data infrastructure				
	7.0203	Manifold area				
	7.0204	Facility control room				
	7.0205	Dehydration units				
	7.0206	Pump Motors				
	7.0207	Compressor units				
	7.0208	Wellheads (injection/withdrawal)				
	7.0209	Storage Tanks				
	7.0210	Regulators/pressure control				
	7.0211	Other (describe)				
R	7.0300	Has a Security Vulnerability Assessments (SVA) or equivalent been conducted at the facility? The assessment should address any vital components.	A - No B - Unknown C - Yes D - Partial; not all SVA steps addressed E - Partial; not all pipeline assets addressed F - Other (describe)			
	7.0400	Is the facility a newly identified critical facility, a newly constructed critical facility, or a critical facility with significant modifications?	A - No B - Unknown C - Yes			
R	7.0500	If yes to Question 7.0400, has an SVA or equivalent been conducted within 12 months of designation or after achieving operational status?	A - No B - Unknown C - Yes			
R	7.0600	Are SVA's or equivalent conducted on periodic basis, not to exceed 36 months?	A - No B - Unknown C - Yes			
R	7.0700	Are appropriate findings implemented within 24 months of the completion of each SVA?	A - No B - Unknown C - Yes			

R	7.0800	Have security tests and audits been conducted at the facility in accordance with the Corporate Security Plan? If yes, select all that apply.	A - No B - Unknown C - Yes			
	7.0801	Internal non-security personnel	Select With "X" In Green Cells			
	7.0802	Internal security professionals				
	7.0803	External government agencies				
	7.0804	External security professionals				
	7.0805	Other (describe)				
	7.0900	Are security audits conducted on an established schedule?	A - No B - Unknown C - Yes, annually or more frequently D - Yes, every two years E - Yes, every three years or less frequently			
	7.1000	Question Removed. Space Reserved for Future Use.		X		Question Removed. Space Reserved for Future Use.
	7.1100	Question Removed. Space Reserved for Future Use.		X		Question Removed. Space Reserved for Future Use.
	7.1200	Are spare vital components available within 24 hours to support emergency restoration of service?	A - No B - Unknown C - Yes D - Partial			
	7.1300	Estimated time to restore temporary/emergency service (i.e., minimally productive volumes) from a worst-case scenario?	A - Unknown B - Less than one day C - 1-5 days D - 6-15 days E - 16-30 days F - 30+ days			
SAI	**8.0000**	**Risk Analysis and Assessments - Cyber**				
	8.0001	There are no CFSR questions related to this SAI.	N/A		**N/A**	
SAI	**9.0000**	**Drills & Exercises**				
R	9.0100	Do facility personnel conduct or participate in annual security drills or exercises to include announced or unannounced tests of security and incident plans? These can be conducted in conjunction with other required drills or exercises.	A - No B - Unknown C - Yes			
R	9.0200	Has the operator developed and implemented a written post-event report assessing security drills or exercises and documenting corrective actions?	A - No B - Unknown C - Yes			
	9.0300	Does the operator invite representatives from law enforcement agencies to participate in security drills and exercises?	A - No B - Unknown C - Yes, representatives invited but did not attend D - Yes, representatives invited and attended			
SAI	**10.0000**	**Cyber Security**				

	10.0100	Does this facility house critical pipeline cyber assets (e.g., SCADA, PCS, DCS measurement and telemetry systems)?	A - No B - Unknown C - Yes			
R	10.0200	In addition to the perimeter security, do you employ additional physical controls to protect cyber assets? Check below.	A - No B - Unknown C - Yes			
	10.0201	None	Select With "X" In Green Cells			
	10.0202	Secured Room/Cabinets				
	10.0203	Proximity card reader				
	10.0204	CCTV Camera				
	10.0205	IDS System				
	10.0206	Other				
R	10.0300	Do you employ more stringent identity and access management practices (e.g., authenticators, password-construct) to protect access into the systems?	A - No B - Unknown C - Yes			
SAI	**11.0000**	**Physical Security & Access Control**				
	11.0100	Are security personnel deployed at the facility? For example, is a guard posted at the main gate to support access control and monitoring?	A - No B - Unknown C - Yes, but not 24/7 D - Yes, 24/7			
	11.0200	Describe security personnel. Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.0201	Company employees				
	11.0202	Contractors (Securitas, Wackenhut, etc.)				
	11.0203	Armed Security				
	11.0204	Off-duty law enforcement personnel				
	11.0205	Unknown				
	11.0206	N/A				
	11.0207	Other (describe)				
	11.0300	Does the operator or facility maintain a contract with a commercial guard company that ensures rapid availability of security personnel in a crisis?	A - No B - Unknown C - Yes			
R	11.0400	Are visitors escorted or monitored while at the facility?	A - No B - Unknown C - Yes			
R	11.0500	Does the facility provide a security perimeter that impedes unauthorized access to the facility or critical areas by installing and maintaining barriers?	A - No B - Unknown C - Yes			
R	11.0600	To impede unauthorized vehicle access, are barriers readily available or deployed on the facility's perimeter, near access control points, and/or near vital components (e.g., fences, bollards, jersey barriers, or equivalent)?	A - No B - Unknown C - Yes			
	11.0700	Select all types of vehicle barriers.	Select With "X" In Green Cells		ZZZ	
	11.0701	Jersey barriers				

	11.0702	Bollards	[redacted]			
	11.0703	Natural barriers (ditch, large rocks, trees)				
	11.0704	Guard rails				
	11.0705	Heavy equipment				
	11.0706	Steel cable				
	11.0707	N/A				
	11.0708	Other (describe)				
	11.0800	Is perimeter fencing installed at the facility?	A - No B - Unknown C - Yes			
	11.0900	Select the type(s) of perimeter fencing material(s). Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.0901	Chain link	[redacted]			
	11.0902	Wood				
	11.0903	Cinder block or brick				
	11.0904	Sheet metal				
	11.0905	No-climb mesh				
	11.0906	Combination of above				
	11.0907	N/A				
	11.0908	Other (describe)				
	11.1000	Is a barbed wire or razor wire topper installed on perimeter fencing?	A - No B - Unknown C - Yes D - Partial			
	11.1100	Including the barbed wire or razor wire topper, what is the approximate overall height of perimeter fencing (as measured when standing on the outside of the fence)? If fencing varies in height, select the height of the shortest section.	A - Under 5-feet B - 6-feet C - 7-feet D - 8-feet E - Over 8-feet			
R	11.1200	Does the perimeter fencing, or barriers fully enclose the facility's vital components?	A - No B - Unknown C - Yes			
	11.1300	Are two layers of fencing installed around the facility's vital component(s)?	A - No B - Unknown C - Yes D - Partial			
R	11.1400	Is there a clear zone of several feet on either side of the fence that is free of obstructions, vegetation, or objects that could be used for concealment or to scale the fence?	A - No B - Unknown C - Yes			
R	11.1500	Does damage, disrepair, erosion, or gaps degrade the security effectiveness of the perimeter gate or fence?	A - No B - Unknown C - Yes			
R	11.1600	Are the gates installed and maintained at the facility of an equivalent quality to the barrier to which they are attached?	A - No B - Unknown C - Yes D - Other (describe)			

	11.1700	Do personnel monitor motorized gates until they close?	A - No B - Unknown C - Yes D - Other (describe)			
R	11.1800	Can emergency egress gates (e.g. Push bar type) be manipulated and opened from outside the fence?	A - No B - Unknown C - Yes			
R	11.1900	Does the facility ensure all perimeter gates are closed and secured when not in use?	A - No B - Unknown C - Yes			
R	11.2000	Are key control procedures established and documented for key tracking, issuance, collection, and loss and unauthorized duplication?	A - No B - Unknown C - Yes			
R	11.2100	Does your facility conduct key inventories every 24 months?	A - No B - Unknown C - Yes, every 24 months or more frequently D - Yes, but not on an established schedule			
R	11.2200	Does the facility utilize a restricted key/blank, patent key/blank, or other form of smart key/electronic access to the critical facility to prevent unauthorized duplication? (Keys stamped do not duplicate would not meet the above criteria.)	A - No B - Unknown C - Yes			
	11.2300	Which groups have keys to padlocks on perimeter gates? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.2301	Company employees				
	11.2302	Long-term, trusted contractors				
	11.2303	Other Contractors				
	11.2304	Pipeline operators or utilities that share the site				
	11.2305	Visitors				
	11.2306	Emergency Responders				
	11.2307	Unknown				
	11.2308	Key distribution is not tracked				
	11.2309	N/A				
	11.2310	Others (describe)				
	11.2400	Are padlocks from other entities daisy-chained with company padlocks on perimeter gates?	A - No B - Unknown C - Yes			

R	11.2500	Are “No Trespassing,” “Authorized Personnel Only,” or signs of similar meaning posted at intervals that are visible from any point of potential entry?	A - No B - Unknown C - Yes, in a manner that is visible from all approaches D - Partial, only at access control points E - Partial, not in a manner that is visible from all approaches F - Other (describe)			
	11.2600	Are electronic access control systems installed at the facility or restricted areas within a facility?	A - No B - Unknown C - Yes			
	11.2700	Which access points are controlled by the electronic access control system? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.2701	Perimeter vehicle gates				
	11.2702	Interior vehicle gates				
	11.2703	Pedestrian gates				
	11.2704	Exterior doors to facility buildings				
	11.2705	Interior doors at facility buildings that lead to sensitive areas				
	11.2706	Other (describe)				
	11.2707	N/A				
	11.2708	Unknown				
	11.2800	Select the type(s) of authentication required by the system(s). Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.2801	Proximity card reader				
	11.2802	Keypad/PIN Code				
	11.2803	Wireless/remote gate opener				
	11.2804	Physical key				
	11.2805	Biometric				
	11.2806	N/A				
	11.2807	Unknown				
	11.2808	Other (describe)				
	11.2900	Does the system log access by authorized personnel?	A - No B - Unknown C - Yes			
	11.3000	Does the system record access attempts by unauthorized personnel?	A - No B - Unknown C - Yes			
	11.3100	Does the system alert employees to access attempts by unauthorized personnel?	A - No B - Unknown C - Yes			
	11.3200	Are access control records periodically reviewed to ensure compliance with policies and procedures?	A - No B - Unknown C - Yes			

	11.3300	Other than employees who are assigned to the facility, which groups have authorized access to perimeter gates that utilize electronic access controls? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.3301	Company employees not assigned to the facility				
	11.3302	Long-term, trusted contractors				
	11.3303	Other Contractors				
	11.3304	Pipeline operators or utilities that share the site				
	11.3305	Visitors				
	11.3306	Emergency Responders				
	11.3307	Unknown				
	11.3308	N/A				
	11.3309	None				
	11.3310	Others (describe)				
	11.3400	Describe access controls for Company employees or long-term trusted contractors not assigned to the facility, if applicable.	E - Describe			
R	11.3500	Does the facility employ security measures to impede unauthorized persons from gaining access to a facility, and restricted areas within a facility? If yes, select all that apply.	A - No C - Yes			
	11.3501	None	Select With "X" In Green Cells			
	11.3502	Verbal screening				
	11.3503	Visual screening				
	11.3504	Validate identification at access control point				
	11.3505	Scheduled appointments				
	11.3506	Verification with visitor's employer				
	11.3507	Proximity card reader				
	11.3508	Physical Key				
	11.3509	Keypad/PIN Code				
	11.3510	Intrusion Detection System (IDS)				
	11.3511	Unknown				
	11.3512	Other (describe)				
R	11.3600	Does the facility implement procedures such as manual or electronic sign in/out) for controlling access to the facility and restricted buildings or areas within the facility?	A - No B - Unknown C - Yes			
R	11.3700	Does the facility employ security measures to monitor, detect, and assess unauthorized access to the facility, within the facility and around critical areas of the facility 24 hours a day, 7 days a week?	A - No B - Unknown C - Yes D - Partial			
	11.3800	Is a CCTV system installed at the facility?	A - No B - Unknown C - Yes			

	11.3900	Is the CCTV system fully functional?	A - No B - Unknown C - Yes			
	11.4000	How many total cameras are installed?	A - 1 B - 2-3 C - 4-6 D - 7+ F - Unknown			
	11.4100	How many of the installed cameras offer pan-tilt-zoom (PTZ) capability?	A - 1 B - 2-3 C - 4-6 D - 7+ F - Unknown G - None			
	11.4200	Where are video images displayed?	Select With "X" In Green Cells		ZZZ	
	11.4201	At the facility				
	11.4202	Remotely at pipeline control center				
	11.4203	Remotely at a security control center				
	11.4204	Remotely at a third party monitoring service				
	11.4205	Remotely at another Company facility				
	11.4206	Unknown				
	11.4207	Not displayed				
	11.4208	N/A				
	11.4209	At another location (describe)				
	11.4300	Select all enhanced capabilities of the camera system.	Select With "X" In Green Cells		ZZZ	
	11.4301	Motion-activated alerts				
	11.4302	Motion-activated recording				
	11.4303	Video analytics				
	11.4304	IR Illumination				
	11.4305	None				
	11.4306	N/A				
	11.4307	Unknown				
	11.4308	Other (describe)				
	11.4400	Does the CCTV system monitor or record activity around vital components?	A - No B - Unknown C - Yes			
	11.4500	Does the CCTV system enable personnel to screen visitors prior to granting entry?	A - No B - Unknown C - Yes			
	11.4600	To support incident response, can real-time video feeds be monitored off-site by those with valid log-in credentials?	A - No B - Unknown C - Yes			

	11.4700	How many days of video imagery are stored before they are deleted or recorded over?	A - 0 B - Unknown C - 1-14 D - 15-30 E - 31-45 F - 45-60 G - 61+			
	11.4800	Did the review team review image quality from the CCTV cameras?	A - No B - Yes, imagery was generally excellent C - Yes, imagery was acceptable D - Yes, imagery was generally poor			
	11.4900	Is there an electronic intrusion detection system (IDS) installed at the facility?	A - No B - Unknown C - Yes			
	11.5000	Is the IDS fully functional?	A - No B - Unknown C - Yes			
	11.5100	What types of sensors are installed and operational? Select all that apply.	Select With "X" In Green Cells		ZZZ	
	11.5101	Microwave				
	11.5102	Mechanical switches				
	11.5103	Magnetic contacts				
	11.5104	N/A				
	11.5105	Passive infrared (PIR)				
	11.5106	Unknown				
	11.5107	Fence disturbance sensors				
	11.5108	Other (describe)				
	11.5200	Does a siren, horn, or similar device broadcast IDS alarms across the facility in a manner that alerts personnel of a potential security event?	A - No B - Unknown C - Yes			
	11.5300	Does the frequency of false or nuisance alarms impact the effectiveness of the IDS system?	A - No B - Unknown C - Yes			
R	11.5400	Does the lighting at the facility provide sufficient illumination for human or technological recognition of intrusion into the facility perimeter or critical areas?	A - No B - Unknown C - Yes D - Partial			
SAI	12.0000	**Personnel Security**				
R	12.0100	Does the facility have an identification and badging policy for personnel who have access to secure areas or sensitive information? Policy should address lost or stolen identification cards or badges, temporary badges, and personnel termination.	A - No B - Unknown C - Yes			

R	12.0200	Does the facility ensure personnel identification cards, or badges are secure from tampering, and contain the individuals photograph and name?	A - No B – Unknown C - Yes D - Other (describe)			
R	12.0300	Does the facility ensure that company or vendor identification is available for examination by being visibly displayed or carried by personnel while on-site?	A - No B – Unknown C - Yes D - Other (describe)			
SAI	13.0000	**Equipment Maintenance and Testing**				
R	13.0100	Has the operator developed and implemented a maintenance program to ensure security systems are in good working order?	A - No B - Unknown C - Yes			
R	13.0200	Does the operator verify the proper operation and/or condition of all security equipment through routine use or quarterly examination?	A - No B - Unknown C - Yes D - Partial, not all security equipment and/or not on a quarterly basis			
R	13.0300	Does the operator identify and respond to security equipment malfunctions or failures in a timely manner?	A - No B - Unknown C - Yes			
R	13.0400	Does the facility provide an equivalent level of protective security measures to mitigate risk during power outages, security equipment failure, or extended repair of security systems?	A - No B - Unknown C - Yes			
	13.0500	If alternate power sources are used to mitigate risks during power outages, are they tested on a quarterly basis?	A - Monthly or more frequently B - Quarterly C - Twice per year D - Annually or less frequently E - No established schedule G - Unknown			
SAI	14.0000	**Recordkeeping**				
R	14.0100	Has the facility developed and documented recordkeeping policies and procedures for security information? Is SSI information being protected in accordance with the provisions of 49 CFR Parts 15 and 1520. (e.g.. locked in a file cabinet or desk when not in use).	A - No B - Unknown C - Yes			
	14.0200	Question Removed. Space Reserved for Future Use.		X		Question Removed. Space Reserved for Future Use.
R	14.0300	Does the operator retain all security testing and audit documents until superseded or replaced?	A - No B - Unknown C - Yes			

	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
Enter Previous CFSR Implementation >>>															

If this is a Pipeline CFSR Revisit, please enter the level of implementation **"R" scores only** from the previous CFSR for 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	Overall
Enter Previous CFSR Recommendations >>>															0

If this is a Pipeline CFSR Revisit, please enter the number of CFSR Recommendations made for each SAI.

DO NOT MODIFY OR ENTER ANY DATA ON THIS SHEET!

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Pipeline Operator Overview

R FY2022 V.1 PRA Draft (February 2

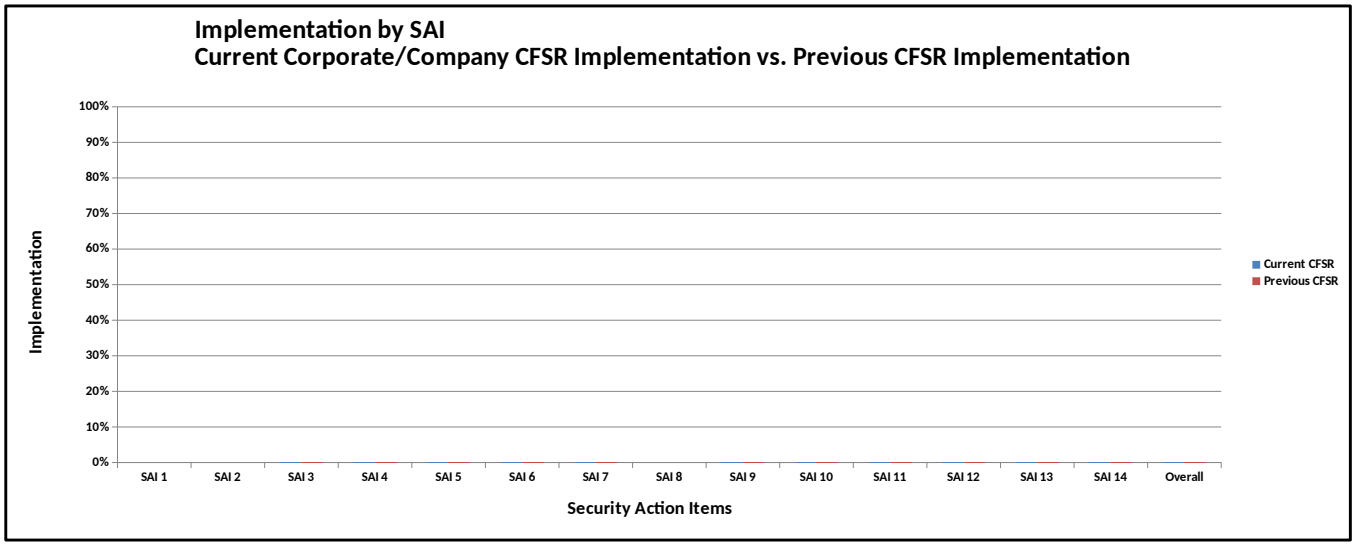
Facility Name		Lead Inspector:	0
0		Assessment Date:	2/26/2021

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION	Implementation	R Only	# of Recommendations
1	Security Plans	N/A	N/A	0
2	Security Plans - Cyber	N/A	N/A	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	N/A	N/A	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%	0.00%	0

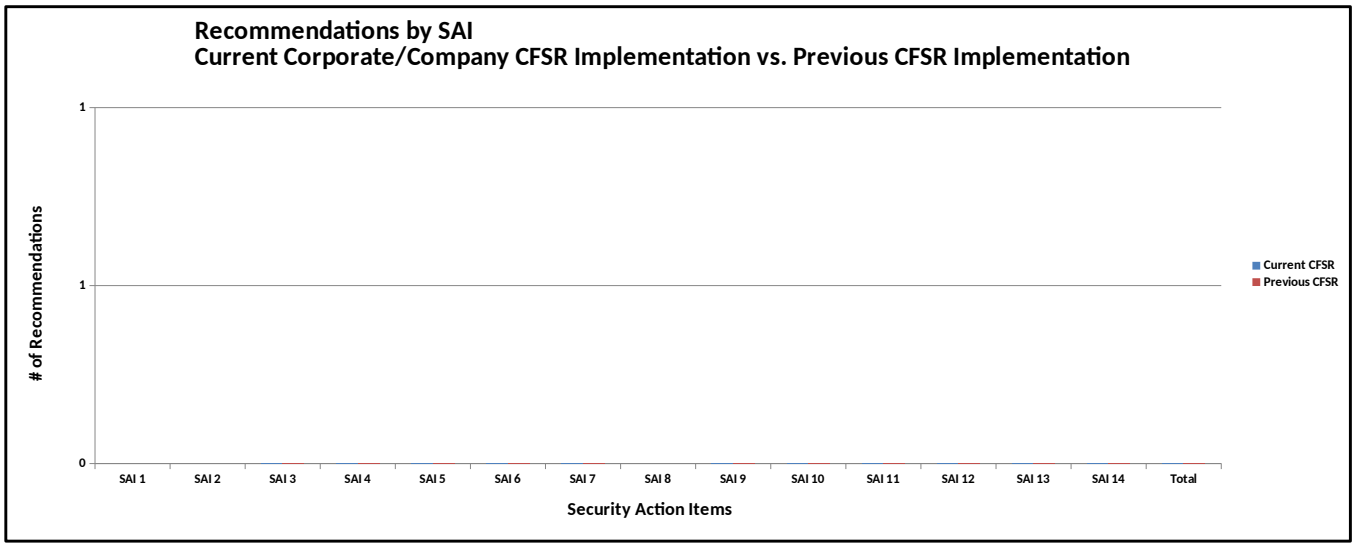
Color Key:

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 CFSR vs. Previous CFSR 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 Corporate/Company CFSR Implementation	N/A	N/A	0%	0%	0%	0%	0%	N/A	0%	0%	0%	0%	0%	0%	0%
Previous Corporate/Company CFSR Implementation	N/A	N/A	0%	0%	0%	0%	0%	N/A	0%	0%	0%	0%	0%	0%	0%
Difference	N/A	N/A	0%	0%	0%	0%	0%	N/A	0%	0%	0%	0%	0%	0%	0%



0															
Current CFSR vs. Previous CFSR 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 Corporate/Company CFSR Recommendations	N/A	N/A	0	0	0	0	0	N/A	0	0	0	0	0	0	0
Previous Corporate/Company CFSR Recommendations	N/A	N/A	0	0	0	0	0	N/A	0	0	0	0	0	0	0
Difference	N/A	N/A	0	0	0	0	0	N/A	0	0	0	0	0	0	0



0
Comments
(List general comments, strengths, and noteworthy practices of the facility's security program)

0			
Recommendations			
These recommendations identify where…			
Recommendation #	**CFSR Question #**	**SAI Description**	**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			

0			
Considerations			
Consideration #	**CFSR Question #**	**SAI Description**	**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			
#	**CFSR Question #**	**SAI Description**	**Best Practice Description**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

0

Photographs

(Place any additional photographs here)

0

Meeting Attendees

Date: 2/26/2021

TSA Pipeline Security Attendees

Name	Title	Division	Name	Title	Division

Pipeline Operator Attendees

Name	Title	Division	Name	Title	Division

Other Attendees

Name	Title	Organization / Company	Name	Title	Organization / Company

CFSR 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

Definitions

Criteria for Critical Facilities

According to the TSA Pipeline Security Guidelines, pipeline facilities meeting one or more of the criteria belov considered to be critical:

A facility or combination of facilities that, if damaged or destroyed, would have the potential to:

1. Disrupt or significantly reduce required service or deliverability to installations identified as critical to nation defense;
2. Disrupt or significantly reduce required service or deliverability to key infrastructure (such as power plants airports) resulting in major economic disruption;
3. Cause mass casualties or significant health effects;
4. Disrupt or significantly reduce required service or deliverability resulting in a state or local government's ina provide essential public services and emergency response for an extended period of time;
5. Significantly damage or destroy national landmarks or monuments;
6. Disrupt or significantly reduce the intended usage of major rivers, lakes, or waterways. (For example, publi water for large populations or disruption of major commerce or public transportation routes);
7. Disrupt or significantly reduce required service or deliverability to a significant number of customers or indi an extended period of time;
8. Significantly disrupt pipeline system operations for an extended period of time (i.e., business critical facilitie

Security Vulnerability Assessments (SVA)

A security vulnerability assessment (SVA) is one of the risk assessment methodologies pipeline operators ma choose. The SVA serves as a planning and decision support tool to assist security managers with identifying evaluating, and prioritizing risks; and determining effective security measures to mitigate threats and vulneral their critical facilities. Common steps performed while conducting an SVA include:

1. Asset Characterization - identification of hazards and consequences of concern for the facility, its surrounc its supporting infrastructure; and identification of existing layers of protection;
2. Threats Assessment - description of possible internal and external threats;
3. Security Vulnerability Analysis - identification of potential security vulnerabilities, existing security measure their level of effectiveness in reducing identified vulnerabilities;
4. Risk Assessment - determination of the relative degree of risk to the facility in terms of the expected effect asset and the likelihood of a success of an attack; and
5. Security Measures Analysis - strategies that reduce the probability of a successful attack or reduce the pos degree of success, strategies that enhance the degree of risk reduction, the capabilities and effectiveness of options, and the feasibility of the options.

Security Audits

A security audit is a structured assessment of the operator's implementation of security policies and procedu specific facility. Audits typically include interviews with facility personnel, reviews of security-related documen records, and a facility inspection.

Site-Specific Measures

Operators should develop, document, and implement site-specific security measures for each of their critical These measures should be tailored explicitly for each individual facility, with emphasis on specific procedures actions to be taken at different threat levels. On a periodic basis, not to exceed 18 months, these facility spec measures should be reviewed and updated as necessary.

Security Inspections

Security inspections are the examination of physical and electronic security measures to ensure that they are delivering the designed security benefit to the facility. Additionally, security inspections should document sign disrepair or damage to security measures, vandalism or theft of property, and indications of criminal, terrorist suspicious activity.

w are

al

or major

ability to

ic drinking

viduals for

es).

ay
,
bilities to

dings, and

s, and

on each

ssible
mitigation

res at a
ts and

facilities.
s and
cific

s of
, or

PAPERWORK REDUCTION ACT STATEMENT: TSA is collecting this information on facility security policies, proc
physical security measures. This is a volunatary collection of information. TSA estimates that the total average bu
response associated with this collection is approximately 4 hours. If you have any comments regarding this form,
ATTN: TSA PRA Officer, TSA-11, PRA 1652-0050, 6595 Springfield Center Drive, Springfield, VA 20598-6011. An ag
conduct or sponsor, and persons are not required to respond to, a collection of information unless it displays a cur
control number. The OMB number for this for is 1652-0050, which expires 11/31/2021.