DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

PIPELINE SECURITY
CRITICAL FACILITY SECURITY REVIEW (CFSR)

INSTRUCTIONS: This form will be used by TSA personnel and their representatives to collect information on critical pipeline infrastructure during a Critical Facility Security Review.

SECTION I. Facility Information

	Topic or Question	Answers	Comments
	General Facility Information		
1.	Date of Review		
2.	Pipeline Company		
3.	Pipeline System		
4.	Pipeline Facility		
5.	Facility Street Address		
6.	City		
7.	State		
8.	County		
9.	Zip Code		
10.	Latitude (N)		
11.	Longitude (W)		
12.	Primary Corporate Security Point of Contact		
13.	Name		
14.	Title		
15.	Office Phone		
16.	Mobile Phone		
17.	E-mail		
18.	Personnel Interviewed		
19.	Name		
20.	Title		
21.	Office Phone		
22.	Mobile Phone		
23.	E-mail		
24.	Name		
25.	Title		
26.	Office Phone		
27.	Mobile Phone		
28.	E-mail		
29.	Name		
30.	Title		
31.	Office Phone		
32.	Mobile Phone		
33.	E-mail		
34.	TSA Review Team		
35.	Name		
36.	Title		
37.	Name		
38.	Title		
39.	Name		
40.	Title		
41.	Name		
42.	Title		

	Topic or Question	Answers	Comments
43.	Observers (e.g., DOT, law enforcement, other operators)		
44.	Primary Commodity Category:	Crude Oil Refined Products Natural Gas/LNG NGL/LPG Toxic Inhalation Hazard (TIH)	
45.	Primary Facility Function(s):	Gas Compressor Station Liquids Pump Station Natural Gas City Gate/Town Border Station Pipeline Interconnect Meter/Regulator Station Mainline Valve Site Bridge Span NGL/LPG Terminal Security Operations Center Pipeline Control Center Back-up Pipeline Control Center Marketing Terminal Underground Storage (note capacity) Above Ground Storage Tanks (note capacity) LNG Peak Shaving Facility Toxic Inhalation Hazard (TIH) Facility Other (describe)	
46.	Is the facility staffed?	No Yes	
47.	Staffing periods?	24/7 7 days/week (days only) Monday-Friday, days and nights Monday-Friday, days only Monday-Friday, partial N/A Other (describe) Varies with season Unknown	
48.	Total number of personnel who are present at the critical facility during day shifts?	0 1-5 6-15 16-25 26-35 36+ N/A Unknown	
49.	Total number of personnel who are present at the critical facility during night/weekend/holiday shifts?	0 1-5 6-15 16-25 26-35 36+ N/A Unknown	
50.	Is the facility a shared site with another pipeline operator, utility, or commercial entity?	No Yes Unknown	

	Topic or Question	Answers	Comments
51.	Is the facility located within the perimeter of another company's or operator's facility?	No Yes Unknown	
52.	Is the facility located within the secured perimeter of a military base?	No Yes Unknown	
53.	Is the facility regulated by the Maritime Transportation Security Act (MTSA)?	No Yes Unknown	
54.	Is all or part of the facility regulated by the Chemical Facility Anti-Terrorism Standards (CFATS)?	No Yes Unknown	
55.	Note general operational characteristics such as number and diameter of inbound/outbound pipelines, volumes of gas or liquids transported and/or stored, and acreage inside perimeter fencing.		
56.	Describe the most significant impact on downstream and upstream customers and interdependent infrastructure if the facility is inoperable.		
	Risk Analysis and Assessments		
57.	Which components are most vital to the facility's continued operations? Select all that apply.	Electrical power infrastructure (substation, switchgear, etc.) Computer/data infrastructure Manifold area Facility control room Dehydration units Pump motors Compressor units Wellheads (injection/withdrawal) Storage tanks Regulators/pressure control Other (describe)	
58.	Are spare vital components available within 24 hours to support emergency restoration of service?	No Unknown Yes Partial N/A	
59.	Estimated time to restore temporary/emergency service (i.e., minimally productive volumes) from a worst case scenario?	Unknown Less than one day 1-5 days 6-15 days 16-30 days 30 + days	
60.	Estimated reconstruction cost if facility is destroyed (in millions of dollars):	Unknown $0 less than $10M $10M - $100M $100M - $500M $500M - $750M Greater than $750M	

	Topic or Question	Answers	Comments
61.	Estimated daily loss of revenue if facility is temporarily inoperable:	Unknown Less than $50,000 $50,000 - $100,000 $100,000-$150,000 $150,000- $200,000 Greater than $200,000	
62.	Based on the criteria presented in the TSA Pipeline Security Guidelines, why is the facility designated “critical?” Select all that apply.	Criterion 1 Criterion 2 Criterion 3 Criterion 4 Criterion 5 Criterion 6 Criterion 7 Criterion 8 Other (describe)	See definitions in Section V.
63.	Have security vulnerability assessments (SVA) been conducted at the facility?	No Unknown Yes Partial; not all SVA steps addressed Partial; not all pipeline assets addressed Other (describe)	See definitions in Section V.
64.	Are SVAs conducted on an established schedule?	No Unknown Yes, every three years or more frequently Yes, every four years Yes, every five years or less frequently N/A	
65.	Are appropriate findings implemented within 18 months of the completion of each SVA?	No Unknown Yes N/A	
66.	Have security audits been conducted at the facility?	No Unknown Yes, with internal non-security personnel Yes, with internal security professionals Yes, with external government agencies Yes, with external security professionals Other (describe)	See definitions in Section V.
67.	Are security audits conducted on an established schedule?	No Unknown Yes, annually or more frequently Yes, every two years Yes, every three years or less frequently N/A	
	Site-Specific Measures		
68.	Are security measures and procedures correlated to the DHS National Terrorism Advisory System (NTAS)?	No Unknown Yes N/A	

	Topic or Question	Answers	Comments
69.	Have site-specific security measures and procedures been developed for the facility?	No Unknown Yes N/A	See definitions in Section V.
70.	Are site-specific security measures and procedures reviewed and updated as necessary on a periodic basis not to exceed 18 months?	No Unknown Yes N/A	
	Public Awareness		
71.	Do the operator's public awareness outreach efforts near this facility include security topics?	No Unknown Yes N/A	
72.	Which public awareness outreach efforts include security topics? Select all that apply.	Public awareness mailings Operator's corporate web site Local public meetings Direct contact at residences and commercial facilities Other (describe) N/A	
	Equipment Maintenance and Testing		
73.	Are scheduled inspections of security measures conducted in order to detect damage, disrepair, tampering, etc.?	No Unknown Yes N/A	See definitions in Section V.
74.	Does the operator have a maintenance program to ensure that the facility's security equipment and systems are in good working order?	No Unknown Yes N/A	
75.	Does the operator verify the proper operation and/or condition of all security equipment on a quarterly basis?	No Unknown Yes Partial, not all security equipment and/or not on a quarterly basis N/A	
76.	Does the operator conduct annual inventories of security equipment?	No Unknown Yes N/A	
77.	Does the facility maintain alternate power sources (for example, generators or battery back-up) or equivalent equipment to minimize interruption of security equipment operation?	No, alternate power sources are not available No, alternate power sources are available but do not support security systems Unknown Partial Yes N/A, there are no electronic security systems at the facility	
78.	How often are alternate power sources tested?	Monthly or more frequently Quarterly Twice per year Annually or less frequently No established schedule N/A Unknown	
	Topic or Question	**Answers**	**Comments**

	Security Incident Response		
79.	Note security incidents or suspicious activity at the facility in the previous five years.		
80.	Note names of nearby law enforcement agencies (LEA).		
81.	Has the facility maintained ongoing coordination/interaction with nearby law enforcement agencies on security topics?	No Unknown Yes N/A	
82.	How often does the facility coordinate/interact with nearby law enforcement agencies on security topics?	Annually or more frequently Every 2-3 years Every 4-5 years Every six years or less frequently Unknown N/A	
83.	Has the facility maintained ongoing coordination/interaction with neighboring pipeline facilities, refineries, and similar facilities on security topics such as coordinated responses to various threat conditions?	No Unknown Yes N/A	
84.	Are emergency contact lists printed and/or readily accessible to facility employees?	No Unknown Yes N/A	
85.	Are bomb threat response checklists printed and readily accessible near facility telephones?	No Unknown Yes N/A	
	Personnel Identification and Badging		
86.	Are photo identification badges issued to company employees who are assigned to the facility?	No Unknown Yes N/A	
87.	Which of the following groups are issued identification badges when at the facility? Select all that apply.	None Company employees not assigned to the facility Long-term, trusted contractors Other contractors Transient visitors (UPS, FedEx, waste disposal, etc.) Others (describe) Unknown N/A	
88.	Which of the following groups are required to display identification badges when at the facility? Select all that apply.	None Company employees assigned to the facility Company employees not assigned to the facility Long-term, trusted contractors Other contractors Transient visitors (UPS, FedEx, waste disposal, etc.) Others (describe) Unknown N/A	
	Topic or Question	**Answers**	**Comments**

	Access Control Procedures		
89.	Are any contractors given the same access privileges as employees?	No Unknown Yes N/A	
90.	What steps are taken to authenticate those without authorized access? Select all that apply.	None Verbal screening Visual screening ID check at access control point Scheduled appointments Verification with visitor's employer Other (describe) Unknown	
91.	Which of the following groups are required to sign a facility log that documents the date/time/purpose of their visit? Select all that apply.	None Company employees assigned to the facility Company employees not assigned to the facility Long-term, trusted contractors Other contractors Transient visitors (UPS, FedEx, waste disposal, etc.) Others (describe) Unknown N/A	
92.	Which of the following groups are escorted or monitored while at the facility? Select all that apply.	None Company employees not assigned to the facility Long-term, trusted contractors Other contractors Transient visitors (UPS, FedEx, waste disposal, etc.) Others (describe) Unknown N/A	
	Personnel Training		
93.	Do facility employees receive initial security awareness training in either a computer-based or classroom format?	No Unknown Yes, classroom Yes, computer-based Yes, both formats Other (describe) N/A	
94.	Does the security awareness training include information from TSA developed training materials?	No Unknown Yes N/A	
95.	Do facility personnel receive periodic refresher training on security awareness topics?	No Unknown Yes, classroom Yes, computer-based Yes, both formats Other (describe) N/A	
	Topic or Question	**Answers**	**Comments**

96.	What is the frequency of refresher training?	Annually or more frequently Every 1-2 years Every three years or less frequently N/A Unknown	
97.	Does the operator maintain security training records?	No Unknown Yes N/A	
	Exercises and Drills		
98.	Do facility personnel conduct or participate in periodic security drills or exercises?	No Unknown Yes N/A	
99.	How often do facility personnel conduct or participate in security drills or exercises?	N/A Unknown Annually or more frequently Every two years Every three years or less frequently Not on an established schedule Other (describe)	
100.	Does the operator develop and implement a written post-exercise report assessing security exercises and documenting corrective actions?	No Unknown Yes N/A	
101.	Does the operator invite representatives from law enforcement agencies to participate in security drills and exercises?	No Unknown Yes, representatives invited but did not attend Yes, representatives invited and attended N/A	
	Guard Force		
102.	Are security personnel deployed at the facility during baseline threat conditions? For example, is a guard posted at the main gate to support access control and monitoring?	No Unknown Yes, but not 24/7 Yes, 24/7	
103.	Describe security personnel. Select all that apply.	Company employees Contractors (Securitas, Wackenhut, etc.) Off-duty law enforcement personnel Other (describe) Unknown N/A	
104.	What percentage of security personnel carry a firearm?	0% 1-25% 26-50% 51-75% 75+% N/A Unknown	
	Topic or Question	**Answers**	**Comments**

105.	Does the operator or facility maintain a contract with a commercial guard company that ensures rapid availability of security personnel in a crisis?	No Unknown Yes N/A	
	Information Protection		
106.	Are printed copies of sensitive security documents protected from unauthorized access?	No Unknown Yes N/A	
	Barriers – Perimeter Fencing		
107.	Is perimeter fencing installed at the facility?	No Unknown Yes N/A	
108.	Select the type(s) of perimeter fencing material(s). Select all that apply.	Chain-link Wood Cinder block or brick Sheet metal No-climb mesh Combination of above Other (describe) N/A	
109.	Is a barbed wire or razor wire topper installed on perimeter fencing?	No Unknown Yes Partial N/A	
110.	What type of barbed wire and/or razor wire is installed on perimeter fencing? Select all that apply.	Outward facing barbed wire Inward facing barbed wire Y-shaped barbed wire Vertical barbed wire Razor wire Other (describe) N/A	
111.	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.	under 5-feet 6-feet 7-feet 8-feet over 8-feet N/A	
112.	Does perimeter fencing fully enclose the facility's vital components?	No Unknown Yes N/A	
113.	Are two layers of fencing installed around the facility's vital component(s)?	No Unknown Yes N/A	
114.	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 by an intruder to scale the fence?	No Unknown Yes N/A	
	Topic or Question	**Answers**	**Comments**

115.	Does vegetation growth degrade the security effectiveness of the perimeter fence?	No Unknown Yes N/A	
116.	Does damage or disrepair degrade the security effectiveness of the perimeter fence?	No Unknown Yes N/A	
117.	Does erosion, drainage areas, or gaps under the fence degrade the security effectiveness of the perimeter fence?	No Unknown Yes N/A	
	Barriers - Perimeter Gates		
118.	How many perimeter vehicle gates are motorized?	0 1 2-3 4-6 7+ N/A Unknown	
119.	Do personnel monitor motorized gates until they close?	No Unknown Yes Other (describe) N/A	
120.	Do large gaps between gate panels and/or posts degrade the security effectiveness of the barrier? Select all that apply.	No Yes, pedestrian gate(s) Yes, emergency egress gate(s) Yes, manual vehicle gate(s) Yes, motorized vehicle gate(s) N/A	
121.	Does erosion, drainage areas, or gaps under gates degrade the security effectiveness of the barrier? Select all that apply.	No Yes, pedestrian gate(s) Yes, emergency egress gate(s) Yes, manual vehicle gate(s) Yes, motorized vehicle gate(s) N/A	
122.	Does damaged or substandard barbed wire or razor wire on perimeter gates degrade the security effectiveness of the barriers? Select all that apply.	No Yes, pedestrian gate(s) Yes, emergency egress gate(s) Yes, manual vehicle gate(s) Yes, motorized vehicle gate(s) N/A	
123.	Can emergency egress gates be manipulated and opened from outside the fence?	No Unknown Yes N/A	
124.	Are all perimeter gates secured when not in active use?	No Unknown Yes N/A	
	Topic or Question	**Answers**	**Comments**

125.	Which groups have keys to padlocks on perimeter gates? Select all that apply.	Company employees Long-term, trusted contractors Other contractors Pipeline operators or utilities that share the site Transient visitors (UPS, FedEx, waste disposal, etc.) Emergency responders Others (describe) Unknown Key distribution is not tracked N/A	
126.	Are padlocks from other entities daisy-chained with company padlocks on perimeter gates?	No Unknown Yes N/A	
127.	Are keys to padlocks on perimeter gates stamped "Do Not Duplicate" or does the facility utilize restricted key blanks to prevent or deter unauthorized duplication?	No Unknown Yes N/A	
128.	Are key control procedures established and documented for key tracking, issuance, collection, and loss?	No Unknown Yes N/A	
129.	Are periodic key inventories conducted?	No Yes, annually or more frequently Yes, every 24 months Yes every 36 months or less frequently Yes, but not on an established schedule N/A Unknown	
	Barriers - Vehicle Barriers		
130.	Are vehicle barriers installed on the facility's perimeter, near access control points, and/or near vital components?	No Unknown Yes No, but barriers are stored on-site and can be rapidly deployed N/A	
131.	Select all types of installed vehicle barriers.	Jersey barriers Bollards Natural barriers (ditch, large rocks, trees) Guard rails Heavy equipment Steel cable Other (describe) N/A	
132.	Are barriers crash-rated per the standards of the U.S. Department of State?	No Yes, K-12 Yes, K-8 Yes, K-4 N/A Unknown	
	Topic or Question	**Answers**	**Comments**

	Electronic Access Controls		
133.	Are electronic access control systems installed at the facility?	No Unknown Yes N/A	
134.	Which groups have authorized access to perimeter gates that utilize electronic access controls? Select all that apply.	Company employees not assigned to the facility Long-term, trusted contractors Other contractors Pipeline operators or utilities that share the site Transient visitors (UPS, FedEx, waste disposal, etc.) Emergency responders Others (describe) Unknown N/A	
135.	Which access points are controlled by the electronic access control system? Select all that apply.	Perimeter vehicle gates Interior vehicle gates Pedestrian gates Exterior doors to facility buildings Interior doors at facility buildings that lead to sensitive areas Other (describe) N/A Unknown	
136.	Select the type(s) of authentication required by the system(s). Select all that apply.	Proximity card reader Keypad/PIN Code Wireless/remote gate opener Physical key Biometric Other (describe) N/A Unknown	
137.	Does the system log access by authorized personnel?	No Unknown Yes N/A	
138.	Does the system record access attempts by unauthorized personnel?	No Unknown Yes N/A	
139.	Does the system alert employees to access attempts by unauthorized personnel?	No Unknown Yes N/A	
140.	Are access control records periodically audited to ensure compliance with policies and procedures?	No Unknown Yes N/A	
	Intrusion Detection and Monitoring – Video Camera System		
141.	Is a CCTV system installed at the facility?	No Unknown Yes N/A	
142.	Is the CCTV system fully functional?	No Unknown Yes N/A	
	Topic or Question	**Answers**	**Comments**

143.	How many total cameras are installed?	1 2-3 4-6 7+ N/A Unknown	
144.	How many of the installed cameras offer pan-tilt-zoom (PTZ) capability?	1 2-3 4-6 7+ N/A Unknown	
145.	Where are video images displayed?	At the facility Remotely at pipeline control center Remotely at a security control center Remotely at a third party monitoring service Remotely at another Company facility At other location (describe) Not displayed N/A Unknown	
146.	Is the system designed and managed in a manner that provides a 24/7 capability to detect and assess unauthorized access?	No Unknown Yes N/A	
147.	To support incident response, can real-time video feeds be monitored off-site by those with valid log-in credentials?	No Unknown Yes N/A	
148.	Does the CCTV system enable personnel to screen visitors prior to granting entry?	No Unknown Yes N/A	
149.	Does the CCTV system monitor or record activity around vital components?	No Unknown Yes N/A	
150.	Select all enhanced capabilities of the camera system.	Motion-activated alerts Motion-activated recording Video analytics IR illumination Other (describe) None N/A Unknown	
151.	Where are video images recorded? Select all that apply.	Not recorded Unknown At the facility Off-site pipeline control Off-site security control center Other location (describe) N/A	
	Topic or Question	**Answers**	**Comments**

152.	How many days of video imagery are stored before they are deleted or recorded over?	0 Unknown 1-14 15-30 31-45 45-60 61+ N/A	
153.	Did the review team review image quality from the CCTV cameras?	No Yes, imagery was generally excellent Yes, imagery was acceptable Yes, imagery was generally poor N/A	
	Intrusion Detection and Monitoring - Intrusion Detection System (IDS)		
154.	Is an intrusion detection system (IDS) installed at the facility?	No Unknown Yes N/A	
155.	Is the IDS fully functional?	No Unknown Yes N/A	
156.	Is the system designed and managed in a manner that provides a 24/7 capability to detect and assess unauthorized access?	No Unknown Yes N/A	
157.	What types of sensors are installed and operational? Select all that apply.	Microwave Magnetic contacts Passive infrared (PIR) Fence disturbance sensors Mechanical switches Other (describe) N/A Unknown	
158.	Does a siren, horn, or similar device broadcast IDS alarms across the facility in a manner that alerts personnel of a potential security event?	No Unknown Yes N/A	
159.	Does the frequency of false or nuisance alarms impact the effectiveness of the IDS system?	No Unknown Yes N/A	
	Facility Lighting		
160.	Is exterior lighting installed at the facility?	No Unknown Yes N/A	
161.	How is the lighting activated? Select all that apply.	photo cell sensors timer manual motion other (describe) N/A Unknown	
	Topic or Question	**Answers**	**Comments**

162.	Are primary access control points adequately illuminated?	No Unknown Yes Partial N/A	
163.	Are vital components adequately illuminated?	No Unknown Yes Partial N/A	
164.	Does the lighting provide adequate illumination for the CCTV cameras (if installed)?	No Unknown Yes Partial N/A	
	Security Signage		
165.	Are “No Trespassing,” “Authorized Personnel Only,” or signs of similar meaning posted along the perimeter fence?	No Yes, in a manner that is visible from all approaches Partial, only at access control points Partial, not in a manner that is visible from all approaches Other (describe) N/A Unknown	
166.	If a CCTV system is installed, are signs posted warning that the premises are under video surveillance?	No Unknown Yes N/A	

SECTION II. Comments

SECTION III. Recommendations

SECTION IV. Aerial Photograph

SECTION V. Definitions

Criteria for Critical Facilities

According to the TSA Pipeline Security Guidelines, pipeline facilities meeting one or more of the criteria below are 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 national defense;
2. Disrupt or significantly reduce required service or deliverability to key infrastructure (such as power plants or major 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 inability to 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, public drinking 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 individuals for an extended period of time;
8. Significantly disrupt pipeline system operations for an extended period of time (i.e., business critical facilities).

Security Vulnerability Assessments (SVA)
A security vulnerability assessment (SVA) is one of the risk assessment methodologies pipeline operators may 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 vulnerabilities to 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 surroundings, and 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 measures, and 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 on each 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 possible degree of success, strategies that enhance the degree of risk reduction, the capabilities and effectiveness of mitigation 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 procedures at a specific facility. Audits typically include interviews with facility personnel, reviews of security-related documents and records, and a facility inspection.

Site-Specific Measures
Operators should develop, document, and implement site-specific security measures for each of their critical facilities. These measures should be tailored explicitly for each individual facility, with emphasis on specific procedures and actions to be taken at different threat levels. On a periodic basis, not to exceed 18 months, these facility specific 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 signs of disrepair or damage to security measures, vandalism or theft of property, and indications of criminal, terrorist, or suspicious activity.

Paperwork Reduction Act Statement:
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. Transportation Security Administration estimates that the average burden for collection is 4 hours. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: TSA-11, Attention: PRA 1652-0050 601 South 12th Street, Arlington, VA 20598