

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

Visit Date:

Report Date:

1 NAME OF COMPANY/ORGANIZATION

2 ONSITE STREET ADDRESS/P.O BOX	3 CITY	4 COUNTY	5 STATE	6 ZIP
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

7 MAILING STREET ADDRESS/P.O BOX	8 CITY	9 COUNTY	10 STATE	11 ZIP
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

12 NAME OF PRIMARY SECURITY COORDINATOR

PRIMARY SECURITY COORDINATOR CONTACT INFORMATION

13 OFFICE PHONE	14 EXT	15 PAGER
<input type="text"/>	<input type="text"/>	<input type="text"/>

16 MOBILE PHONE	17 FAX
<input type="text"/>	<input type="text"/>

18 EMAIL

19 NAME OF ALTERNATE SECURITY COORDINATOR

ALTERNATE SECURITY COORDINATOR CONTACT INFORMATION

20 OFFICE PHONE	21 EXT	22 PAGER
<input type="text"/>	<input type="text"/>	<input type="text"/>

23 MOBILE PHONE	24 FAX
<input type="text"/>	<input type="text"/>

25 EMAIL

26 24-HOUR EMERGENCY CONTACT PHONE NUMBER

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

COMPANY-WIDE DESCRIPTION:

27 LIST THE STATES IN WHICH YOU ARE OPERATING?

28 TOTAL PIPELINE MILEAGE

29 CROSS-BORDER OPERATION YES NO

30 PRODUCTS CARRIED:

- Refined product
 Crude oil
 Natural Gas
 Liquefied Natural Gases
 Chemicals (List below)

31 NUMBER OF PIPELINE SYSTEMS OPERATED

32 PIPELINE SIZE(S)

33 MAXIMUM DAILY FLOW CAPACITY

34 AVERAGE DAILY FLOW CAPACITY

35 ANNUAL DELIVERIES

36 STORAGE CAPACITY

37 NUMBER OF CUSTOMERS OR DELIVERY FACILITIES

38 TOTAL NUMBER OF CORPORATE EMPLOYEES

39 TOTAL NUMBER OF PIPELINE OPERATIONS EMPLOYEES

54 LIST MEETING ATTENDEES

55 FILLED OUT BY

COMPANY PROFILE:

40 NUMBER OF PIPELINES ON BRIDGES

41 NUMBER OF STANDALONE PIPELINE BRIDGES

42 NUMBER OF STORAGE FACILITIES

43 NUMBER OF BREAKOUT TANK FACILITIES

44 NUMBER OF PUMPING STATIONS

45 NUMBER OF COMPRESSOR STATIONS

46 NUMBER OF LNG FACILITIES

47 NUMBER OF NGL FACILITIES

48 NUMBER OF MARINE TERMINALS

49 NUMBER OF SCADA CONTROL ROOMS

50 NUMBER OF BACKUP SCADA CONTROL ROOMS

51 NUMBER OF EMERGENCY OPERATION CENTERS

52 NUMBER OF CITY GATE STATIONS

53 COMPANY PROFILE COMMENTS



CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

1 Have you established a Corporate Security Program?

2 Does your corporation have a written corporate security plan (or other documented security procedures or policies)?

3 Which of the following corporate plans are directly included or incorporated by reference in the corporate security plan?

- | | |
|---|---|
| <input type="checkbox"/> Business continuity plan | <input type="checkbox"/> Emergency recovery plan |
| <input type="checkbox"/> SCADA plan | <input type="checkbox"/> Site-specific security measures for each critical facility |
| <input type="checkbox"/> Emergency response plan | <input type="checkbox"/> Other (if checked, elaborate in comment field) |

4 Is the corporate security plan reviewed on an annual basis?

5 Is the corporate security plan updated as required?

6 Does the corporate security plan describe the responsibilities and duties of personnel assigned to security functions?

7 Is the corporate security plan readily available for those persons responsible for security actions?



CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

8 Does your corporation provide all employees with a redacted version of your corporate security plan? YES NO

9 Which of the following elements are addressed in the corporate security plan?

- | | |
|---|---|
| <input type="checkbox"/> System Description | <input type="checkbox"/> Security Threat and Incident Response Procedures |
| <input type="checkbox"/> Security Administration and Management Structure | <input type="checkbox"/> HSAS Response Procedures |
| <input type="checkbox"/> Risk Analysis and Assessments | <input type="checkbox"/> Security Plan Reviews and Update |
| <input type="checkbox"/> Physical Security and Access Control | <input type="checkbox"/> Recordkeeping |
| <input type="checkbox"/> Equipment Maintenance and Testing | <input type="checkbox"/> SCADA System Security |
| <input type="checkbox"/> Design and Construction Security Measures | <input type="checkbox"/> Essential Security Contacts |
| <input type="checkbox"/> Personnel Screening | <input type="checkbox"/> Security Testing and Audits |
| <input type="checkbox"/> Communications | <input type="checkbox"/> Resilience or business continuity |
| <input type="checkbox"/> Personnel Training | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Drills and Exercises | |
-

10 Do you have sufficient resources, including trained staff and equipment, to effectively execute your corporate security program? YES NO

11 Have you designated one primary individual, by position or name, to manage the corporate security program? YES NO

12 Have you designated one alternate individual, by position or name to manage the corporate security program in the absence of the primary individual? YES NO



CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

- 13** Does your corporate security manager work 100% on security (as opposed to being tasked with safety, environmental health and safety, compliance, etc.)? YES NO

- 14** Does your corporation's security manager (or equivalent position) have a direct reporting relationship to the senior leadership in the corporation? YES NO

- 15** Does the corporation have a cross-department security committee? YES NO

- 16** Which of the following departments are represented on the security committee?

- | | |
|---|---|
| <input type="checkbox"/> Corporate management | <input type="checkbox"/> Engineering |
| <input type="checkbox"/> Human resources | <input type="checkbox"/> Operations |
| <input type="checkbox"/> Security | <input type="checkbox"/> Information Technology |
| <input type="checkbox"/> Legal | <input type="checkbox"/> Other (if checked, elaborate in comment field) |

- 17** Do you have executive level support for implementing security enhancements? YES NO

- 18** Does your corporation have a dedicated funding mechanism (e.g. capital, operating, and maintenance budget) for security? YES NO



CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

19 How much operating and maintenance money did your corporation spend on security in the previous fiscal year?

- | | |
|---|---|
| <input type="radio"/> < \$99,999 | <input type="radio"/> \$500,000 - \$999,999 |
| <input type="radio"/> \$100,000 - \$249,999 | <input type="radio"/> \$1,000,000 - \$4,999,999 |
| <input type="radio"/> \$250,000 - \$499,999 | <input type="radio"/> >\$5,000,000 |

20 How much capital money did your corporation spend on security in the previous fiscal year?

- | | |
|---|---|
| <input type="radio"/> < \$99,999 | <input type="radio"/> \$500,000 - \$999,999 |
| <input type="radio"/> \$100,000 - \$249,999 | <input type="radio"/> \$1,000,000 - \$4,999,999 |
| <input type="radio"/> \$250,000 - \$499,999 | <input type="radio"/> >\$5,000,000 |

? Record the total corporate and corporate security budgets in the comment field

? **21** Does your corporation integrate security measures during the design, construction, renovation, or retrofit of a facility?

22 Does your corporation have an ongoing relationship with the following entities/departments/agencies/organizations?

- | | |
|---|---|
| <input type="checkbox"/> Local emergency responders | <input type="checkbox"/> Local homeowners |
| <input type="checkbox"/> Tribal emergency responders | <input type="checkbox"/> Neighboring corporations |
| <input type="checkbox"/> State emergency responders | <input type="checkbox"/> Trade association security committees |
| <input type="checkbox"/> Federal emergency responders | <input type="checkbox"/> Sector coordinating councils |
| <input type="checkbox"/> Federal Bureau of Investigation (FBI) | <input type="checkbox"/> American Society of Industrial Security (ASIS) |
| <input type="checkbox"/> Department of Homeland Security (DHS) | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Transportation Security Administration (TSA) | |

? **23** Does your corporation actively verify and update external contact lists annually?



CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

24 Does your corporation utilize any of the following security standards or methodologies?

- National Fire Protection Association (NFPA)
- International Standards Organization (ISO)
- American Society of Industrial Security (ASIS)
- American Petroleum Institute/National Petroleum Refiners Association (API/NPRA)
- Interstate Natural Gas Association of America (INGAA)
- American Gas Association (AGA)
- Other (if checked, elaborate in comment field)

? **25** Has your corporation established security metrics and/or internal reporting?

? **26** Does your corporation employ a centralized security operations center?

? **27** Are security incidents at your corporation managed centrally?

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

CORPORATE SECURITY PROGRAM MANAGEMENT:

Corporate Security Program Management general comments:

[Empty box for general comments]



RISK ANALYSIS - CRITICAL FACILITY DETERMINATION:

YES NO

1 Does your corporation utilize a documented process to determine which facilities are critical within your pipeline systems, not exceeding eighteen months? YES NO

2 Does your corporation protect and limit access to criticality assessments and critical facility lists? YES NO

3 Who has access to the list of critical facilities?

- Corporate management
- Security Manager
- Assistant Security Manager
- Security Staff
- Critical facility managers
- Other facility managers
- All employees
- Outside entity who assisted in criticality assessment
- Other (if checked, elaborate in comment field)

4 Did you utilize the criteria from TSA's Pipeline Security Guidelines to determine your list of critical facilities? YES NO

RISK ANALYSIS - SECURITY VULNERABILITY ASSESSMENT (SVA):

5 Does your corporation conduct documented Threat Assessments? YES NO



RISK ANALYSIS

YES NO

6 Does your corporate threat-assessment process assess the following potential threats?

- | | |
|--|---|
| <input type="checkbox"/> Trespassing | <input type="checkbox"/> Terrorism |
| <input type="checkbox"/> Bomb threat | <input type="checkbox"/> Active shooter |
| <input type="checkbox"/> Arson | <input type="checkbox"/> Chemical, biological, radiological or nuclear incident |
| <input type="checkbox"/> Riot | <input type="checkbox"/> Cyber incident |
| <input type="checkbox"/> Suspicious incident | <input type="checkbox"/> Insider threat |
| <input type="checkbox"/> Crime or vandalism | <input type="checkbox"/> Hostage |
| <input type="checkbox"/> Surveillance | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |

7 From whom does your corporation receive threat information to assist in your SVA?

- | | |
|---|---|
| <input type="checkbox"/> Transportation Security Operations Center (TSOC) | <input type="checkbox"/> Local law enforcement |
| <input type="checkbox"/> Protective Security Advisory (PSA) | <input type="checkbox"/> Coast Guard |
| <input type="checkbox"/> Joint Terrorism Task Force (JTTF) | <input type="checkbox"/> Broadcast news media |
| <input type="checkbox"/> Federal Bureau of Investigation (FBI) | <input type="checkbox"/> Corporate |
| <input type="checkbox"/> Homeland Security Information Network (HSIN) | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> State fusion center(s) | |

8 Does your corporation conduct an SVA of your critical facilities periodically, not exceeding 36 months? YES NO

9 When conducting an SVA, which of the following documented methodologies are you using?

- Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER)
- American Petroleum Institute/ National Petroleum Refiners Association (API/NPRA)
- Mission, Symbolism, History, Accessibility, Recognizability, Population, Proximity (MSHARRPP)
- Third-party or corporate proprietary
- Other (if checked, elaborate in comment field)



RISK ANALYSIS

YES NO

? **10** Does your corporation conduct an SVA of your critical facilities after completing any significant enhancement or modification, not exceeding twelve months? YES NO

? **11** Does your corporation conduct SVAs on your non-critical facilities? YES NO

? **12** Are facility support infrastructure (i.e. water, electrical power, and telecommunications) considered during the SVA? YES NO

? **13** Are the findings and recommendations from SVAs reviewed at the executive level? YES NO

? **14** Upon completion of an SVA, are corrective actions implemented within eighteen months? YES NO

? **15** Does your corporation protect and limit access to SVAs? YES NO



RISK ANALYSIS

16 Who in your corporation has access to completed SVAs?

- | | |
|---|---|
| <input type="checkbox"/> Corporate management | <input type="checkbox"/> Other facility managers |
| <input type="checkbox"/> Security Manager | <input type="checkbox"/> All employees |
| <input type="checkbox"/> Assistant Security Manager | <input type="checkbox"/> Outside entity who assisted in the SVAs |
| <input type="checkbox"/> Other Security Personnel | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Critical facility managers | |

Risk Analysis general comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

OPERATIONAL SECURITY:

YES NO

1 Is there at least one individual within your corporation who holds a current federal security clearance? YES NO

2 What is the highest level of clearance that is held within your corporation?

- Top Secret Confidential
 Secret Other (if checked elaborate in comment field)

3 Does your corporation have a process to receive, store, and disseminate restricted or classified information? YES NO

4 Does your corporate policy stipulate that external communications such as press releases, marketing information, and other publicly available information be reviewed for security concerns prior to release? YES NO

5 Does your corporation regularly review your corporate website to ensure potentially sensitive, excessive detail, or confidential information is not publicly available that could pose a security risk? YES NO

6 Does your corporation have a process to control documents that, taken together, may provide an adversary with operational or security information that could harm the company? YES NO

7 Does your corporation have a document marking policy or procedure? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

OPERATIONAL SECURITY:

YES NO

8 Has your corporation taken any of the following steps to apply operational security ("OPSEC") in daily activities?

- | | |
|--|--|
| <input type="checkbox"/> Mark documents | <input type="checkbox"/> Dispose of computer equipment and associated media securely |
| <input type="checkbox"/> Hold conversations in appropriate locations | <input type="checkbox"/> Create strong passwords |
| <input type="checkbox"/> Report undue interest in pipeline security or operations | <input type="checkbox"/> Change passwords periodically |
| <input type="checkbox"/> Secure sensitive documents outside of offices areas (such as in vehicles or in transport) | <input type="checkbox"/> Vary patterns of behavior |
| <input type="checkbox"/> Dispose of documents properly | <input type="checkbox"/> Remove badges in public |
| | <input type="checkbox"/> Other (if checked, elaborate in comment field) |

Operational Security general comments:



PERSONNEL AND CONTRACTOR SECURITY:

YES NO

1 Does your corporation conduct pre-employment background checks on all your potential employees? YES NO

2 Does your corporation conduct different levels of pre-employment background checks based on the nature of the position? YES NO

3 Which of the following types of pre-employment background checks does your corporation conduct?

Criminal Alcohol/drug screen
 DMV Employment verification
 Credit Other (if checked elaborate in comment field)

4 Does your corporation conduct recurring background checks every ten years (or less) for employees occupying security positions or who have access to sensitive information or areas? YES NO

5 Do your corporate contracts require background checks for all contractor personnel who have unescorted or unsupervised access to company critical facilities? YES NO

6 Does your corporation verify that background checks, of at least the same degree of rigor as corporate checks, are performed for the following persons who have unescorted or unsupervised access to company critical facilities?

Contractors Tenants
 Vendors Other (if checked, elaborate in comment field)
 Other co-located facility personnel



PERSONNEL AND CONTRACTOR SECURITY:

YES NO

7 Does your corporation have a policy and/or procedure in place for secure employee termination?

8 Which of the following are conducted during termination activities?

- | | |
|---|--|
| <input type="checkbox"/> Retrieve badge or identification card or badge | <input type="checkbox"/> Block computer-system access |
| <input type="checkbox"/> Disable passwords | <input type="checkbox"/> Discharged employee signs nondisclosure agreement |
| <input type="checkbox"/> Retrieve keys | <input type="checkbox"/> Other (if checked elaborate in comment field) |
| <input type="checkbox"/> Retrieve operational and/or security manuals | |

Personnel and Contractor Security general comments:



PHYSICAL ASSET PROTECTION - PHYSICAL SECURITY MEASURES:

YES NO

1 Does your corporation use a layered, defense-in-depth, system of physical security measures? YES NO

2 Which of the following features or processes are in use at your critical facilities?

- | | |
|--|--|
| <input type="checkbox"/> Fences | <input type="checkbox"/> Patrols |
| <input type="checkbox"/> Gates | <input type="checkbox"/> Lighting |
| <input type="checkbox"/> Signage (i.e. No trespassing, Do Not Enter, Authorized Personnel Only, CCTV in use, etc.) | <input type="checkbox"/> Crime prevention through environmental design (CPTED) |
| <input type="checkbox"/> Closed circuit television (CCTV) | <input type="checkbox"/> Unarmed guards |
| <input type="checkbox"/> Intrusion sensors | <input type="checkbox"/> Armed guards |
| <input type="checkbox"/> Alarms | <input type="checkbox"/> Video analytic systems |
| <input type="checkbox"/> Cleared zones around fence lines | <input type="checkbox"/> Video recording |
| <input type="checkbox"/> Locks | <input type="checkbox"/> Intrusion detection systems |
| <input type="checkbox"/> Barriers (i.e. bollards, planters or jersey barriers) | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Tamper devices | |

3 Which of the following features are in use at your non-critical facilities?

- | | |
|--|--|
| <input type="checkbox"/> Fences | <input type="checkbox"/> Patrols |
| <input type="checkbox"/> Gates | <input type="checkbox"/> Lighting |
| <input type="checkbox"/> Signage (i.e. No trespassing, Do Not Enter, Authorized Personnel Only, CCTV in use, etc.) | <input type="checkbox"/> Crime prevention through environmental design (CPTED) |
| <input type="checkbox"/> Closed circuit television (CCTV) | <input type="checkbox"/> Unarmed guards |
| <input type="checkbox"/> Intrusion sensors | <input type="checkbox"/> Armed guards |
| <input type="checkbox"/> Alarms | <input type="checkbox"/> Video analytic systems |
| <input type="checkbox"/> Cleared zones around fence lines | <input type="checkbox"/> Video recording |
| <input type="checkbox"/> Locks | <input type="checkbox"/> Intrusion detection systems |
| <input type="checkbox"/> Barriers (i.e. bollards, planters or jersey barriers) | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Tamper devices | |

4 Does your corporate policy stipulate that doors, gates, windows, or entrances be closed and locked when not in use? YES NO



PHYSICAL ASSET PROTECTION - PHYSICAL SECURITY MEASURES:

YES NO

? **5** Does your corporation have 24/7 security monitoring at your critical facilities to detect and assess unauthorized access?

? **6** Does your corporate policy stipulate that any facility lighting must provide sufficient illumination for human or technological recognition of an intrusion?

Physical Asset Protection - Physical Security Measures general comments:



PHYSICAL ASSET PROTECTION - ACCESS:

YES NO

1 Does your corporation have an access control policy?

2 To what areas does your corporation's access control policy apply?

- | | |
|--|---|
| <input type="checkbox"/> Critical field facilities | <input type="checkbox"/> Security offices |
| <input type="checkbox"/> Non-critical field facilities | <input type="checkbox"/> Server rooms |
| <input type="checkbox"/> Headquarters facility | <input type="checkbox"/> Specific operational areas |
| <input type="checkbox"/> SCADA Control Center | <input type="checkbox"/> Other (If checked, elaborate in comment field) |

3 How is your corporation physically controlling normal access to restricted areas?

- | | |
|---|--|
| <input type="checkbox"/> Lock and key | <input type="checkbox"/> Proximity card |
| <input type="checkbox"/> Biometric reader | <input type="checkbox"/> Radio remote control |
| <input type="checkbox"/> Digital key card | <input type="checkbox"/> Other (if checked elaborate in comment field) |

4 Does your corporate access control policy address access to restricted areas for visitors, transient visitors, and emergency responders?

5 Do corporate personnel escort visitors while at restricted areas or critical facilities?

6 To whom does your corporation allow unescorted access to restricted areas?

- | | |
|---|---|
| <input type="checkbox"/> Company employees not assigned to the facility | <input type="checkbox"/> Visitors |
| <input type="checkbox"/> Contractors assigned to the facility | <input type="checkbox"/> Emergency responders in emergency situations |
| <input type="checkbox"/> Contractors not assigned to the facility | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Transient visitors (UPS, Fed-Ex, USPS workers, vending machine suppliers, landscapers, etc.) | |



PHYSICAL ASSET PROTECTION - ACCESS:

YES NO

7 Does your corporation track, document, or digitally record access to restricted areas? YES NO

8 Does your corporation have a badging or identification card policy? YES NO

9 To whom does your corporation issue badges or identification cards?

<input type="checkbox"/> All employees	<input type="checkbox"/> Contractors not assigned to the facility
<input type="checkbox"/> Company employees assigned to the facility	<input type="checkbox"/> Visitors
<input type="checkbox"/> Company employees not assigned to the facility	<input type="checkbox"/> Other (If checked, elaborate in comment field)
<input type="checkbox"/> Contractors assigned to the facility	

10 Does your corporation have policies and procedures to address lost or stolen badges or identification cards? YES NO

11 Does your corporation have a corporate key-control program? YES NO

12 Does your corporation use patent keys to prevent unauthorized duplication? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

PHYSICAL ASSET PROTECTION - ACCESS:

Risk Analysis - Threat Assessment general comments:

[Empty rectangular box for Risk Analysis - Threat Assessment general comments]

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SCADA SECURITY:

YES NO

1 Does your corporation have a written SCADA security plan or other documented security procedures or policies? YES NO

2 Does your corporation have policies and/or procedures in place to track changes made to the SCADA systems? YES NO

3 Does your corporation review and assess all its SCADA security procedures annually? YES NO

4 Does your corporation have procedures in place to prevent unauthorized access to your SCADA system(s)? YES NO

5 Does your corporation conduct penetration testing on your SCADA network? YES NO

6 Does your corporation have a designated individual responsible for SCADA security? YES NO

7 Can your corporation's SCADA system be controlled remotely? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SCADA SECURITY:

YES NO

? **8** Does your corporation perform a SCADA system(s) criticality assessment at least every eighteen months?

? **9** Does your corporation perform a vulnerability assessment on your SCADA system(s) at least every 36 months?

? **10** Does your corporation utilize a layered, defense-in-depth, approach to SCADA system(s) access?

? **11** Is your corporation's SCADA system(s) housed on a isolated/segregated secure network?

? **12** Does your corporation monitor and periodically review SCADA system(s) network connections, including remote and third-party connections?

? **13** Prior to deployment, does your corporation evaluate the security risks of using wireless networking in your environment?



SCADA SECURITY:

YES NO

14 Which of the following features does your corporation use to secure your SCADA system(s)?

- | | |
|---|---|
| <input type="checkbox"/> Locked facilities | <input type="checkbox"/> Access lists |
| <input type="checkbox"/> Strong passwords | <input type="checkbox"/> Entry logs |
| <input type="checkbox"/> Communication gateways | <input type="checkbox"/> Firewalls |
| <input type="checkbox"/> Access control lists | <input type="checkbox"/> De-Militarized Zone (DMZ) |
| <input type="checkbox"/> Authenticators | <input type="checkbox"/> Intrusion detection system |
| <input type="checkbox"/> Separation of duties | <input type="checkbox"/> Intrusion prevention system |
| <input type="checkbox"/> Least privilege (Able to access only information and resources that are necessary) | <input type="checkbox"/> Maintain patches |
| <input type="checkbox"/> Key cards | <input type="checkbox"/> Other (if checked, elaborate in comment field) |

? **15** Has your corporation developed a cross-functional cyber security team for information security between your SCADA systems and enterprise networks?

16 Which of the following groups are represented on your corporate cyber security team?

- | | |
|--|--|
| <input type="checkbox"/> Operations | <input type="checkbox"/> Third-party contractors or vendors |
| <input type="checkbox"/> Information Technology (IT) | <input type="checkbox"/> Other (if checked elaborate in comment field) |

? **17** Has your corporation established security standards for evaluating the acquisition of SCADA system devices and equipment?

? **18** Does your corporation only use SCADA workstations for approved control system activities?

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SCADA SECURITY:

YES NO

? 19 Does your corporation securely dispose of the hardware used to run your SCADA system(s)?

? 20 Does your corporation incorporate restoration and recovery of your SCADA system(s) in your resiliency plans?

SCADA Security general comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SECURITY TRAINING:

YES NO

- 1** Does your corporation require and conduct security-awareness training upon hire for all employees and contractors? YES NO

- 2** Does your corporation require and conduct biennial refresher security-awareness training for all employees and contractors? YES NO

- 3** Does your corporation require and conduct job-specific security training for all employees assigned security duties? YES NO

- 4** Does your corporation require and conduct annual refresher job-specific security training for all employees assigned security duties? YES NO

- 5** Does your corporation maintain security-related training records? YES NO

- 6** Does your corporation conduct security orientations for visitors and vendors? YES NO

- 7** Does your corporation conduct SCADA system(s) security training? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SECURITY TRAINING:

YES NO

8 Does your corporation conduct annual refresher training for SCADA system(s) security? YES NO

9 To maintain security domain awareness, do your corporation's security personnel attend conferences, forums, or other advanced security training? YES NO

10 Which of the following training opportunities or affiliations have your corporation's security personnel availed themselves of?

<input type="checkbox"/> Security forums or conferences	<input type="checkbox"/> Government sector committee(s)
<input type="checkbox"/> Pipeline forums or conferences	<input type="checkbox"/> Industry security collaboration
<input type="checkbox"/> Advanced security training	<input type="checkbox"/> Other (if checked elaborate in comment field)
<input type="checkbox"/> Participate in security committee(s)	

11 Does your corporation use any of TSA's security training materials? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SECURITY TRAINING:

Security Training general comments:

[Empty text box for security training general comments]

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

DRILL, EXERCISE AND PROGRAM VALIDATION:

YES NO

1 Does your corporation conduct annual security-related drills and exercises?

2 Over the past three (3) years, what types of facilities in your corporation have you exercised?

- | | |
|--|--|
| <input type="checkbox"/> Critical facility | <input type="checkbox"/> Security operations center |
| <input type="checkbox"/> Non-critical facility | <input type="checkbox"/> MTSA facility |
| <input type="checkbox"/> SCADA center | <input type="checkbox"/> Other (if checked elaborate in comment field) |
| <input type="checkbox"/> Emergency operations center | |

3 Over the past three (3) years, with whom has your corporation exercised?

- | | |
|---|--|
| <input type="checkbox"/> Local emergency responders | <input type="checkbox"/> DHS |
| <input type="checkbox"/> Tribal emergency responders | <input type="checkbox"/> TSA |
| <input type="checkbox"/> State emergency responders | <input type="checkbox"/> Neighboring corporations |
| <input type="checkbox"/> Federal emergency responders | <input type="checkbox"/> Other (if checked elaborate in comment field) |
| <input type="checkbox"/> FBI | |

4 Does your corporation conduct unannounced security-related drills or exercises?

5 Does your corporation document and maintain the results of all security-related drills and exercises?

6 Does your corporation document and complete corrective actions identified during security-related drills and exercises?

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

DRILL, EXERCISE AND PROGRAM VALIDATION:

YES NO

7 Does your corporation test and evaluate communications equipment annually?

8 Does your corporation validate its security contact list periodically?

9 Does your corporation conduct periodic security audits of its facilities?

Drill, Exercise and Program Validation general comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

MAINTENANCE:

YES NO

1 Does your corporation have a security equipment maintenance program?

2 Which of the following methods does your corporate security maintenance program utilize?

- Corrective maintenance Testing
 Preventive maintenance Inspection

3 Does your corporation conduct quarterly security equipment inspections?

4 Does your corporation conduct an annual security equipment inventory?

5 Does your corporation have alternate power sources for security equipment at critical facilities?

6 Does your corporation perform periodic operability checks on communication devices used in a security-related incident response?

7 Does your corporation retain security equipment maintenance and testing records?

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

MAINTENANCE:

Maintenance general comments:



COMMUNICATIONS DEVICES AND MECHANISMS:

YES NO

1 Which of the following devices does your corporation use to accomplish emergency/security communication or notification?

- | | |
|--|--|
| <input type="checkbox"/> Email | <input type="checkbox"/> Low band radio |
| <input type="checkbox"/> Telephone | <input type="checkbox"/> High band radio |
| <input type="checkbox"/> Cellular telephone | <input type="checkbox"/> Company band radio |
| <input type="checkbox"/> Satellite telephone | <input type="checkbox"/> Pager |
| <input type="checkbox"/> Video conferencing | <input type="checkbox"/> Other (if checked elaborate in comment box) |

? **2** Does your corporation have a mechanism, computer driven process or vender service for automatic security notifications?

? **3** Does your corporation use Government Emergency Telephone System (GETS) cards?

Communications Devices and Mechanisms general comments:



SECURITY INCIDENT MANAGEMENT:

YES NO

- 1** Does your corporation maintain a list of internal contact information for reporting and responding to a security incident, threat, or suspicious activity? YES NO

- 2** Which of the following internal contacts is on the corporation security incident, threat, or suspicious activity notification list?

- | | |
|--|---|
| <input type="checkbox"/> Corporate management | <input type="checkbox"/> All employees |
| <input type="checkbox"/> Security management | <input type="checkbox"/> Contractors |
| <input type="checkbox"/> Critical facility employees | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |

- 3** Which of the following external agencies/organizations is on the corporation security incident, threat or suspicious activity notification list?

- | | |
|--|---|
| <input type="checkbox"/> National Response Center | <input type="checkbox"/> Other Federal agencies |
| <input type="checkbox"/> Local emergency responders/911 | <input type="checkbox"/> Federal Bureau of Investigation (FBI) |
| <input type="checkbox"/> Transportation Security Administration/Transportation Security Operations Center (TSA/TSOC) | <input type="checkbox"/> Department of Homeland Security (DHS) |
| <input type="checkbox"/> Tribal emergency responders | <input type="checkbox"/> Neighboring corporations |
| <input type="checkbox"/> State emergency responders | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |

- 4** During periods of heightened HSAS threat conditions, would your corporation implement enterprise-wide graduated security measures that correspond to the threat level? YES NO

- 5** During periods of heightened HSAS threat conditions, would your corporation implement site-specific graduated security measures that correspond to the threat level? YES NO



SECURITY INCIDENT MANAGEMENT:

YES NO

6 Does your corporation have a policy and/or procedure for internally disseminating security threat or incident information? YES NO

7 To whom in your corporation is security threat or incident information disseminated?

- | | |
|---|---|
| <input type="checkbox"/> Corporate management | <input type="checkbox"/> Engineering |
| <input type="checkbox"/> Security management | <input type="checkbox"/> Operations |
| <input type="checkbox"/> Regional operations management | <input type="checkbox"/> Union representative |
| <input type="checkbox"/> Site management | <input type="checkbox"/> Tenants |
| <input type="checkbox"/> Internal security committee | <input type="checkbox"/> Contractors |
| <input type="checkbox"/> Human resources | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |
| <input type="checkbox"/> Legal | |

8 From whom does your corporation receive current security threat information?

- | | |
|---|---|
| <input type="checkbox"/> Transportation Security Operations Center (TSOC) | <input type="checkbox"/> Coast Guard |
| <input type="checkbox"/> Protective Security Advisory (PSA) | <input type="checkbox"/> Broadcast news media |
| <input type="checkbox"/> Joint Terrorism Task Force (JTTF) | <input type="checkbox"/> Corporate affiliations |
| <input type="checkbox"/> Federal Bureau of Investigation (FBI) | <input type="checkbox"/> Department of Energy |
| <input type="checkbox"/> Homeland Security Information Network (HSIN) | <input type="checkbox"/> Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) |
| <input type="checkbox"/> State fusion center(s) | <input type="checkbox"/> Other (if checked, elaborate in comment field) |
| <input type="checkbox"/> Local law enforcement | |

9 Does your corporation have a policy and/or procedure to record security threat information received? YES NO

10 Does your corporation have a policy and/or procedure to evaluate security threat information as it is received? YES NO



SECURITY INCIDENT MANAGEMENT:

YES NO

- 11** Does your corporation have adequate staffing to implement security measures in response to security threat information? YES NO

- 12** Does your corporation have contracts in place with private security providers to augment existing security staff during times of heightened alert? YES NO

- 13** During times of heightened alert, would your corporation limit physical access to critical facilities? YES NO

- 14** During times of heightened alert, would your corporation limit physical access to non-critical facilities? YES NO

- 15** During times of HSAS Level Orange alert, would your corporation enact the following physical access controls at your critical facilities?

- | | |
|---|---|
| <input type="checkbox"/> Limit facility access to essential personnel | <input type="checkbox"/> Delay or reschedule non-vital capital project work that could affect facility security |
| <input type="checkbox"/> Limit facility access to essential visitors | <input type="checkbox"/> Increase lighting of facility buffer zones |
| <input type="checkbox"/> Limit facility access to essential vehicles | <input type="checkbox"/> Verify operating conditions of security systems (i.e. intrusion detection, cameras, or lighting) |
| <input type="checkbox"/> Limit facility access to essential contractors | <input type="checkbox"/> Request additional police patrols around the facility |
| <input type="checkbox"/> Increase surveillance of critical areas and facilities | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |
| <input type="checkbox"/> Restrict deliveries to those essential to continued operations | |
| <input type="checkbox"/> Conduct random inspections of vehicles | |
| <input type="checkbox"/> Delay or reschedule non-vital maintenance activities that could affect facility security | |



SECURITY INCIDENT MANAGEMENT:

16 During times of HSAS Red alert, would your corporation enact the following physical access controls at your critical facilities?

- | | |
|---|---|
| <input type="checkbox"/> Cancel or delay contractor work and services | <input type="checkbox"/> Erect barriers and/or obstacles to control vehicular traffic flow |
| <input type="checkbox"/> Allow deliveries by appointment only | <input type="checkbox"/> Restrict vehicle parking to 150 feet from all critical areas and assets |
| <input type="checkbox"/> Inspect all briefcases, bags, purses, or backpacks | <input type="checkbox"/> Coordinate with local authorities regarding closing nearby public roads and facilities |
| <input type="checkbox"/> Inspect all vehicles prior to entering the facility | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |
| <input type="checkbox"/> Inspect all deliveries including packages and cargo | |
| <input type="checkbox"/> Close non-essential entrances and facility access points | |
| <input type="checkbox"/> Staff and monitor active facility entrances and access points 24/7 | |

17 During times of HSAS Orange alert, would your corporation enact any of the following measures on your SCADA systems?

- | | |
|--|---|
| <input type="checkbox"/> Increase monitoring of intrusion detection systems on your SCADA network? | <input type="checkbox"/> Report any unusual SCADA system network activity |
| <input type="checkbox"/> Remind personnel to be vigilant regarding suspicious electronic mail | <input type="checkbox"/> Other (If checked elaborate in comment field) |

18 During times of HSAS Red alert, would your corporation enact any of the following measures on your SCADA systems?

- | |
|---|
| <input type="checkbox"/> Limit network communications links to essential sites / users |
| <input type="checkbox"/> Review and revoke any credentials that are not current and necessary |
| <input type="checkbox"/> Other (If checked elaborate in comment field) |



SECURITY INCIDENT MANAGEMENT:

YES NO

19 During times of HSAS Orange alert, would your corporation enact any of the following communication-related steps?

- | | |
|--|--|
| <input type="checkbox"/> Inform all employees and on-site contractors of the increase or decrease to HSAS level Orange | <input type="checkbox"/> Advise local law enforcement of HSAS level Orange security measures |
| <input type="checkbox"/> Conduct security awareness briefings to all employees and on-site contractors | <input type="checkbox"/> Verify operational capability of intelligence and emergency communications networks |
| <input type="checkbox"/> Brief employees and contractors on indicators of suspicious packages or mail | <input type="checkbox"/> Monitor intelligence and emergency communications networks |
| <input type="checkbox"/> Review response procedures for suspicious packages or mail | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |
| <input type="checkbox"/> Inform local law enforcement of the change in HSAS level | |

20 During times of HSAS Red alert, would your corporation enact any of the following communication-related steps?

- | | |
|--|--|
| <input type="checkbox"/> Inform all employees of the increase to HSAS level Red | <input type="checkbox"/> Participate in scheduled situational briefings (e.g. TSA, including local law enforcement, and industry associations) |
| <input type="checkbox"/> Conduct daily security and awareness briefings for each shift | <input type="checkbox"/> Other (If checked elaborate in comment field) |

? **21** Does your corporation utilize an incident management system for security-related events?

? **22** Does your corporation use the National Incident Management System (NIMS)?

23 Does your corporation have procedures for the following types of incidents?

- | | | | |
|--|--|---|---|
| <input type="checkbox"/> Incident reporting | <input type="checkbox"/> Arson | <input type="checkbox"/> Terrorist attack | <input type="checkbox"/> Insider threat |
| <input type="checkbox"/> Homeland Security Advisory System (HSAS) levels | <input type="checkbox"/> Riot | <input type="checkbox"/> Active shooter | <input type="checkbox"/> Hostage |
| <input type="checkbox"/> Trespassing | <input type="checkbox"/> Suspicious incident | <input type="checkbox"/> Chemical, biological, radiological or nuclear incident | <input type="checkbox"/> Crime scene management |
| <input type="checkbox"/> Bomb threat | <input type="checkbox"/> Crime or vandalism | <input type="checkbox"/> Cyber incident | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |
| <input type="checkbox"/> Pandemic | <input type="checkbox"/> Surveillance | | |

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

SECURITY INCIDENT MANAGEMENT:

YES NO

24 Which organizations does your corporation work with during a security incident?

- | | |
|--|---|
| <input type="checkbox"/> Local emergency responders | <input type="checkbox"/> Department of Homeland Security (DHS) |
| <input type="checkbox"/> Tribal emergency responders | <input type="checkbox"/> Transportation Security Administration (TSA) |
| <input type="checkbox"/> State emergency responders | <input type="checkbox"/> Department of Transportation (DOT) |
| <input type="checkbox"/> Federal emergency responders | <input type="checkbox"/> Neighboring corporations |
| <input type="checkbox"/> Federal Bureau of Investigation (FBI) | <input type="checkbox"/> Other (if checked, elaborate in the comment field) |

? **25** Does your corporation have a corporate emergency operations center for use during security incidents?

Security Incident Management general comments:



RESILIENCE:

YES NO

1 Would damage to, or destruction of, a facility or a combination of facilities in your pipeline system have the potential to significantly disrupt operations for greater than 72 hours for any of the following?

- Your system The nation
 A region Across an international border
 A state

2 Has your corporation identified any of the following as critical customers?

- Installations identified as critical to national defense State or local government infrastructure
 Key infrastructure (such as power plants or major airports) Other (if checked elaborate in comment field)

? **3** Has your corporation established lines of delegated authority/succession of security responsibilities?

? **4** Has your corporation established continuity of service plans to ensure continued product availability to critical customers during a security-related event?

5 Has your corporation procured or arranged, in advance, for any of the following to minimize response time for repair or replacement following a security-related event?

- Critical pipe Essential utilities
 Critical fittings UPS/backup generators
 Equipment for repair Other (if checked, elaborate in comment field)

? **6** Does your corporation have adequate personnel to promptly repair and return systems to operation following a security-related event?

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

RESILIENCE:

YES NO

- 7** Does your corporation have mutual aid agreements in place to assist in returning your systems to operation following a security-related event? YES NO

- 8** Does your corporation have standing contracts for emergency pipeline repair following a security-related event? YES NO

- 9** Does your corporation have alternate means of transporting your product if your systems were compromised following a security-related event? YES NO

- 10** Does your corporation have adequate alternate supply to maintain the flow of product following a security-related event? YES NO

- 11** Does your corporation have adequate storage (i.e. breakout tanks, caverns, or LNG tanks) to maintain the flow of product following a security-related event? YES NO

- 12** Does your corporation have a dispersed pipeline system as opposed to a single long-haul transmission line? YES NO

- 13** Does your corporation have adequate financial reserves to redirect funds following a security-related event? YES NO

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

RESILIENCE:

Resilience general comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

FINAL COMMENTS:

? Site or Control Center Visit Notes comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

FINAL COMMENTS:

? Findings and Recommendations comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

FINAL COMMENTS:

? Smart Practices comments:

A large, empty rectangular box intended for entering Smart Practices comments.

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

FINAL COMMENTS:

? Critical Facilities List comments:

PIPELINE CORPORATE SECURITY REVIEW



Transportation
Security
Administration

FINAL COMMENTS:

? References and Other Miscellaneous Notes:

“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 8 hours per year. 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-XXXX 601 South 12th Street, Arlington, VA 20598”