PIPELINE CORPORATE SECURITY REVIEW

SENSITIVE SECURITY INFORMATION

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

7 MAILING STREET ADDRESS/P.O BOX | **8** CITY | **9** COUNTY | **10** STATE | **11** ZIP

12 NAME OF PRIMARY SECURITY COORDINATOR

PRIMARY SECURITY COORDINATOR CONTACT INFORMATION

13 OFFICE PHONE | **14** EXT | **15** PAGER

16 MOBILE PHONE | **17** FAX

18 EMAIL

19 NAME OF ALTERNATE SECURITY COORDINATOR

ALTERNATE SECURITY COORDINATOR CONTACT INFORMATION

20 OFFICE PHONE | **21** EXT | **22** PAGER

23 MOBILE PHONE | **24** FAX

25 EMAIL

26 24-HOUR EMERGENCY CONTACT PHONE NUMBER

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

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

54 LIST MEETING ATTENDEES

55 FILLED OUT BY

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?

- ☐ Business continuity plan
- ☐ SCADA plan
- ☐ Emergency response plan
- ☐ Emergency recovery plan
- ☐ Site-specific security measures for each critical facility
- ☐ 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?

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

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

10 Do you have sufficient resources, including trained staff and equipment, to effectively execute your corporate security program?

11 Have you designated one primary individual, by position or name, to manage the corporate security program?

12 Have you designated one alternate individual, by position or name to manage the corporate security program in the absence of the primary individual?

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.)?

14 Does your corporation's security manager (or equivalent position) have a direct reporting relationship to the senior leadership in the corporation?

15 Does the corporation have a cross-department security committee?

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

- ☐ Corporate management
- ☐ Human resources
- ☐ Security
- ☐ Legal
- ☐ Engineering
- ☐ Operations
- ☐ Information Technology
- ☐ Other (if checked, elaborate in comment field)

17 Do you have executive level support for implementing security enhancements?

18 Does your corporation have a dedicated funding mechanism (e.g. capital, operating, and maintenance budget) for security?

CORPORATE SECURITY PROGRAM MANAGEMENT:

YES NO

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

- ○ < $99,999
- ○ $100,000 - $249,999
- ○ $250,000 - $499,999
- ○ $500,000 - $999,999
- ○ $1,000,000 - $4,999,999
- ○ >$5,000,000

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

- ○ < $99,999
- ○ $100,000 - $249,999
- ○ $250,000 - $499,999
- ○ $500,000 - $999,999
- ○ $1,000,000 - $4,999,999
- ○ >$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?

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

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? ○ ○

CORPORATE SECURITY PROGRAM MANAGEMENT:

Corporate Security Program Management 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? ○ ○

2 Does your corporation protect and limit access to criticality assessments and critical facility lists? ○ ○

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? ○ ○

RISK ANALYSIS - SECURITY VULNERABILITY ASSESSMENT (SVA):

5 Does your corporation conduct documented Threat Assessments? ○ ○

RISK ANALYSIS

YES NO

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

- ☐ Trespassing
- ☐ Bomb threat
- ☐ Arson
- ☐ Riot
- ☐ Suspicious incident
- ☐ Crime or vandalism
- ☐ Surveillance
- ☐ Terrorism
- ☐ Active shooter
- ☐ Chemical, biological, radiological or nuclear incident
- ☐ Cyber incident
- ☐ Insider threat
- ☐ Hostage
- ☐ Other (if checked, elaborate in the comment field)

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

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

8 Does your corporation conduct an SVA of your critical facilities periodically, not exceeding 36 months? ○ ○

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?	○	○
11 Does your corporation conduct SVAs on your non-critical facilities?	○	○
12 Are facility support infrastructure (i.e. water, electrical power, and telecommunications) considered during the SVA?	○	○
13 Are the findings and recommendations from SVAs reviewed at the executive level?	○	○
14 Upon completion of an SVA, are corrective actions implemented within eighteen months?	○	○
15 Does your corporation protect and limit access to SVAs?	○	○

RISK ANALYSIS

16 Who in your corporation has access to completed SVAs?

- ☐ Corporate management
- ☐ Security Manager
- ☐ Assistant Security Manager
- ☐ Other Security Personnel
- ☐ Critical facility managers
- ☐ Other facility managers
- ☐ All employees
- ☐ Outside entity who assisted in the SVAs
- ☐ Other (if checked, elaborate in comment field)

Risk Analysis general comments:

OPERATIONAL SECURITY:

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

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)

	YES	NO
3 Does your corporation have a process to receive, store, and disseminate restricted or classified information?	○	○
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?	○	○
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 ?	○	○
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?	○	○
7 Does your corporation have a document marking policy or procedure?	○	○

OPERATIONAL SECURITY:

YES NO

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

- ☐ Mark documents
- ☐ Hold conversations in appropriate locations
- ☐ Report undue interest in pipeline security or operations
- ☐ Secure sensitive documents outside of offices areas (such as in vehicles or in transport)
- ☐ Dispose of documents properly
- ☐ Dispose of computer equipment and associated media securely
- ☐ Create strong passwords
- ☐ Change passwords periodically
- ☐ Vary patterns of behavior
- ☐ Remove badges in public
- ☐ 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?	○	○
2	Does your corporation conduct different levels of pre-employment background checks based on the nature of the position?	○	○

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

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

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

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

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?

- ☐ Retrieve badge or identification card or badge
- ☐ Disable passwords
- ☐ Retrieve keys
- ☐ Retrieve operational and/or security manuals
- ☐ Block computer-system access
- ☐ Discharged employee signs nondisclosure agreement
- ☐ Other (if checked elaborate in comment field)

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? ○ ○

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

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

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

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

4 Does your corporate policy stipulate that doors, gates, windows, or entrances be closed and locked when not in use? ○ ○

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?

- ☐ Critical field facilities
- ☐ Non-critical field facilities
- ☐ Headquarters facility
- ☐ SCADA Control Center
- ☐ Security offices
- ☐ Server rooms
- ☐ Specific operational areas
- ☐ Other (If checked, elaborate in comment field)

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

- ☐ Lock and key
- ☐ Biometric reader
- ☐ Digital key card
- ☐ Proximity card
- ☐ Radio remote control
- ☐ 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?

- ☐ Company employees not assigned to the facility
- ☐ Contractors assigned to the facility
- ☐ Contractors not assigned to the facility
- ☐ Transient visitors (UPS, Fed-Ex, USPS workers, vending machine suppliers, landscapers, etc.)
- ☐ Visitors
- ☐ Emergency responders in emergency situations
- ☐ Other (if checked, elaborate in comment field)

PHYSICAL ASSET PROTECTION - ACCESS:

YES NO

7 Does your corporation track, document, or digitally record access to restricted areas?

8 Does your corporation have a badging or identification card policy?

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

- All employees
- Company employees assigned to the facility
- Company employees not assigned to the facility
- Contractors assigned to the facility
- Contractors not assigned to the facility
- Visitors
- Other (If checked, elaborate in comment field)

10 Does your corporation have policies and procedures to address lost or stolen badges or identification cards?

11 Does your corporation have a corporate key-control program?

12 Does your corporation use patent keys to prevent unauthorized duplication?

PHYSICAL ASSET PROTECTION - ACCESS:

Risk Analysis - Threat Assessment general comments:

SCADA SECURITY:

	YES	NO
1 Does your corporation have a written SCADA security plan or other documented security procedures or policies?	○	○
2 Does your corporation have policies and/or procedures in place to track changes made to the SCADA systems?	○	○
3 Does your corporation review and assess all its SCADA security procedures annually?	○	○
4 Does your corporation have procedures in place to prevent unauthorized access to your SCADA system(s)?	○	○
5 Does your corporation conduct penetration testing on your SCADA network?	○	○
6 Does your corporation have a designated individual responsible for SCADA security?	○	○
7 Can your corporation's SCADA system be controlled remotely?	○	○

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)?

- ☐ Locked facilities
- ☐ Strong passwords
- ☐ Communication gateways
- ☐ Access control lists
- ☐ Authenticators
- ☐ Separation of duties
- ☐ Least privilege (Able to access only information and resources that are necessary)
- ☐ Key cards
- ☐ Access lists
- ☐ Entry logs
- ☐ Firewalls
- ☐ De-Militarized Zone (DMZ)
- ☐ Intrusion detection system
- ☐ Intrusion prevention system
- ☐ Maintain patches
- ☐ 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?

- ☐ Operations
- ☐ Information Technology (IT)
- ☐ Third-party contractors or vendors
- ☐ 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? ○ ○

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:

SECURITY TRAINING:

	YES	NO
1 Does your corporation require and conduct security-awareness training upon hire for all employees and contractors?	○	○
2 Does your corporation require and conduct biennial refresher security-awareness training for all employees and contractors?	○	○
3 Does your corporation require and conduct job-specific security training for all employees assigned security duties?	○	○
4 Does your corporation require and conduct annual refresher job-specific security training for all employees assigned security duties?	○	○
5 Does your corporation maintain security-related training records?	○	○
6 Does your corporation conduct security orientations for visitors and vendors?	○	○
7 Does your corporation conduct SCADA system(s) security training?	○	○

SECURITY TRAINING:

	YES	NO
8 Does your corporation conduct annual refresher training for SCADA system(s) security?	○	○
9 To maintain security domain awareness, do your corporation's security personnel attend conferences, forums, or other advanced security training?	○	○

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

- ☐ Security forums or conferences
- ☐ Pipeline forums or conferences
- ☐ Advanced security training
- ☐ Participate in security committee(s)
- ☐ Government sector committee(s)
- ☐ Industry security collaboration
- ☐ Other (if checked elaborate in comment field)

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

SECURITY TRAINING:

Security Training general comments:

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?

- Critical facility
- Non-critical facility
- SCADA center
- Emergency operations center
- Security operations center
- MTSA facility
- Other (if checked elaborate in comment field)

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

- Local emergency responders
- Tribal emergency responders
- State emergency responders
- Federal emergency responders
- FBI
- DHS
- TSA
- Neighboring corporations
- Other (if checked elaborate in comment field)

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?

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:

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
- ☐ Preventive maintenance
- ☐ Testing
- ☐ Inspection

	YES	NO
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?	○	○

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?

- ☐ Email
- ☐ Telephone
- ☐ Cellular telephone
- ☐ Satellite telephone
- ☐ Video conferencing
- ☐ Low band radio
- ☐ High band radio
- ☐ Company band radio
- ☐ Pager
- ☐ 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? ○ ○

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

- ☐ Corporate management
- ☐ Security management
- ☐ Critical facility employees
- ☐ All employees
- ☐ Contractors
- ☐ 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?

- ☐ National Response Center
- ☐ Local emergency responders/911
- ☐ Transportation Security Administration/Transportation Security Operations Center (TSA/TSOC)
- ☐ Tribal emergency responders
- ☐ State emergency responders
- ☐ Other Federal agencies
- ☐ Federal Bureau of Investigation (FBI)
- ☐ Department of Homeland Security (DHS)
- ☐ Neighboring corporations
- ☐ 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? ○ ○

5 During periods of heightened HSAS threat conditions, would your corporation implement site-specific graduated security measures that correspond to the threat level? ○ ○

SECURITY INCIDENT MANAGEMENT:

YES NO

6 Does your corporation have a policy and/or procedure for internally disseminating security threat or incident information? ○ ○

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

- ☐ Corporate management
- ☐ Security management
- ☐ Regional operations management
- ☐ Site management
- ☐ Internal security committee
- ☐ Human resources
- ☐ Legal
- ☐ Engineering
- ☐ Operations
- ☐ Union representative
- ☐ Tenants
- ☐ Contractors
- ☐ Other (if checked, elaborate in the comment field)

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

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

9 Does your corporation have a policy and/or procedure to record security threat information received? ○ ○

10 Does your corporation have a policy and/or procedure to evaluate security threat information as it is received? ○ ○

SECURITY INCIDENT MANAGEMENT:

YES NO

11 Does your corporation have adequate staffing to implement security measures in response to security threat information? ○ ○

12 Does your corporation have contracts in place with private security providers to augment existing security staff during times of heightened alert? ○ ○

13 During times of heightened alert, would your corporation limit physical access to critical facilities? ○ ○

14 During times of heightened alert, would your corporation limit physical access to non-critical facilities? ○ ○

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

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

SECURITY INCIDENT MANAGEMENT:

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

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

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

- ☐ Increase monitoring of intrusion detection systems on your SCADA network?
- ☐ Remind personnel to be vigilant regarding suspicious electronic mail
- ☐ Report any unusual SCADA system network activity
- ☐ 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?

- ☐ Limit network communications links to essential sites / users
- ☐ Review and revoke any credentials that are not current and necessary
- ☐ 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?

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

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

- ☐ Inform all employees of the increase to HSAS level Red
- ☐ Conduct daily security and awareness briefings for each shift
- ☐ Participate in scheduled situational briefings (e.g. TSA, including local law enforcement, and industry associations)
- ☐ 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?

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

SECURITY INCIDENT MANAGEMENT:

YES NO

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

- ☐ Local emergency responders
- ☐ Tribal emergency responders
- ☐ State emergency responders
- ☐ Federal emergency responders
- ☐ Federal Bureau of Investigation (FBI)
- ☐ Department of Homeland Security (DHS)
- ☐ Transportation Security Administration (TSA)
- ☐ Department of Transportation (DOT)
- ☐ Neighboring corporations
- ☐ 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
- ☐ A region
- ☐ A state
- ☐ The nation
- ☐ Across an international border

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

- ☐ Installations identified as critical to national defense
- ☐ Key infrastructure (such as power plants or major airports)
- ☐ State or local government infrastructure
- ☐ 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
- ☐ Critical fittings
- ☐ Equipment for repair
- ☐ Essential utilities
- ☐ UPS/backup generators
- ☐ 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? ○ ○

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?	○	○
8 Does your corporation have standing contracts for emergency pipeline repair following a security-related event?	○	○
9 Does your corporation have alternate means of transporting your product if your systems were compromised following a security-related event?	○	○
10 Does your corporation have adequate alternate supply to maintain the flow of product following a security-related event?	○	○
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?	○	○
12 Does your corporation have a dispersed pipeline system as opposed to a single long-haul transmission line?	○	○
13 Does your corporation have adequate financial reserves to redirect funds following a security-related event?	○	○

RESILIENCE:

Resilience general comments:

FINAL COMMENTS:

Site or Control Center Visit Notes comments:

FINAL COMMENTS:

Findings and Recommendations comments:

FINAL COMMENTS:

Smart Practices comments:

FINAL COMMENTS:

Critical Facilities List comments:

FINAL COMMENTS:

References and Other Miscellaneous Notes: