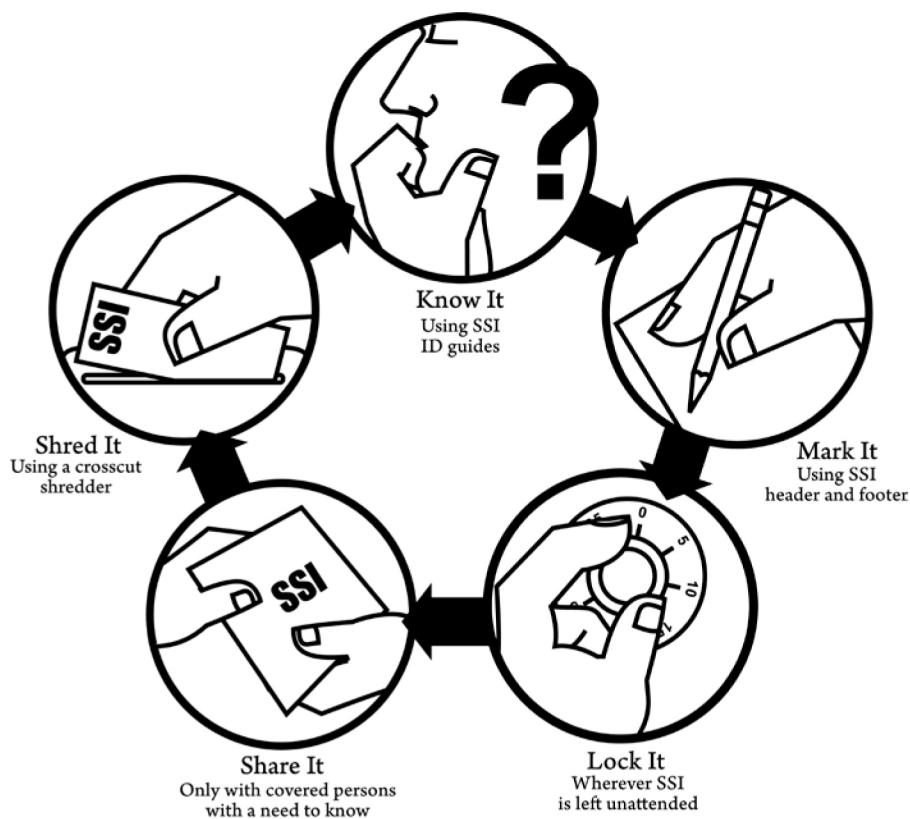


DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet



For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

THIS PAGE INTENTIONALLY LEFT BLANK

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION
DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

PIPELINE SECURITY
CORPORATE SECURITY REVIEW (CSR)

SECTION I. Instructions

PURPOSE

The Corporate Security Review (CSR) is one of TSA's core programs designed to better understand pipeline-operator security planning and implementation. The CSR meeting is designed to help TSA learn more about your company's pipeline system(s) and security and to establish a relationship that will be helpful for your company during any security-related event or emergency. It is also an opportunity to review your company's list of critical facilities and understand the details of your company's security program and plans. If this is a return visit, we will discuss how your company has changed or evolved since our previous visit and also discuss how your company has reduced its risk through evolution, mitigation, and preparation. Please note, the CSR is not a compliance review, audit, or inspection.

ADVANCED PREPARATIONS

Advanced preparations make the meeting much more efficient.

- Please review this question set and fill in your answers before the CSR visit.
- Please be prepared to discuss what your company does to protect its pipeline system(s). Consider both physical and cyber asset-protection measures.

HINTS FOR FILLING OUT THE QUESTION SET

The question set is broken up into several parts. Each part has between 3 and 27 questions.

- There are two basic types of questions:
 - Those that can be answered with a "yes" or "no"
 - Those with a short list of answers where multiple choices may be selected
- Each question has a comment box that can be used to supply supplemental or explanatory information.
- Supplemental information has been provided to help answer the questions. To view this help, hover—do not click—over the small question mark to the left of the question number.

INFORMATION SECURITY

Any information your company provides TSA is considered Sensitive Security Information (SSI) under 5 U.S.C. 552 and 49 CFR parts 15 and 1520. The protections of the rule cover any discussions, observations, and disclosure of records during the course of the review. TSA protects all information shared and will provide your company a non-disclosure agreement on TSA letterhead.

To invoke the protection of the rule, SENSITIVE SECURITY INFORMATION is established in every header and the SSI rule is established in every footer.

SENSITIVE SECURITY INFORMATION

THIS PAGE INTENTIONALLY LEFT BLANK

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

Visit Date: Report Date:

SECTION II. Company Contact Information

1. Name Of Corporation/Company

2. Meeting Street Address 3. City 4. County 5. State 6. Zip

7. Corporate Mailing Address 8. City 9. County 10. State 11. Zip

12. Name Of Primary Security Coordinator

13. Office Phone 14. Ext 15. Pager

16. Mobile Phone 17. Fax

18. Email

19. Name Of Alternate Security Coordinator

20. Office Phone 21. Ext 22. Pager

23. Mobile Phone 24. Fax

25. Email

26. 24-Hour Emergency Contact Phone Number

1. _____ 2. _____ 3. _____

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION III. Company-Wide Description

27. List the states in which you are operating

28. Total pipeline mileage _____

29. Cross-border operations **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. Total number of corporate employees _____

38. Total number of pipeline operations employees

39. Number of pipelines on bridges _____

40. Number of standalone pipeline bridges _____

41. Number of storage facilities _____

42. Number of breakout tank facilities _____

43. Number of pumping stations _____

44. Number of compressor stations _____

45. Number of LNG facilities _____

46. Number of NGL facilities _____

47. Number of marine terminals _____

48. Number of SCADA control rooms _____

49. Number of backup SCADA control rooms _____

50. Number of emergency operations centers _____

51. Number of Delivery Points _____

52. Company Profile Comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IV. 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 | Emergency recovery plan |
| SCADA plan | Site-specific security measures for each critical facility |
| Emergency response plan | Other (if checked, elaborate in comment field) |

? 4. | Is the corporate security plan reviewed on a regular basis and updated as required?

? 5. | Does the corporate security plan describe the responsibilities and duties of personnel assigned to security functions?

? 6. | Is the corporate security plan readily available for those persons responsible for security actions?

? 7. | Does your corporation provide all employees with a redacted version of your corporate security plan?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IV. Corporate Security Program Management *continued*

YES NO

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

- | | |
|--|--|
| System description | Security-threat and incident-response procedures |
| Security administration and management structure | National Terrorism Advisory System (NTAS) measures |
| Risk analysis and assessments | Security plan reviews and updates |
| Physical security and access control | Recordkeeping |
| Equipment maintenance and testing | Supervisory Control and Data Acquisition (SCADA) system security |
| Design and construction security measures | Essential security contacts |
| Personnel screening | Security testing and audits |
| Communications | Resilience or business continuity |
| Personnel training | Other (if checked, elaborate in comment field) |
| Drills and exercises | |

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

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

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

? 12. Does your corporate security manager work 100 percent on security as opposed to being tasked with safety, environmental health and safety, compliance, and so forth?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IV. Corporate Security Program Management *continued*

YES NO

- ?** 13. Does your corporation's security manager or equivalent position have a direct reporting relationship to the senior leadership in the corporation?

- ?** 14. Does the corporation have a cross-departmental security committee?

15. Which of the following departments are represented on the security committee?

- | | |
|----------------------|--|
| Corporate management | Engineering |
| Human resources | Operations and/or maintenance |
| Security | Information technology |
| Legal | Other (if checked, elaborate in comment field) |

- ?** 16. Do you have executive-level support for implementing security enhancements?

- ?** 17. Does your corporation have a dedicated funding mechanism—capital, operating, and/or maintenance budget—for security?

SENSITIVE SECURITY INFORMATION

SECTION IV. Corporate Security Program Management *continued*

YES NO

18. How much operations and/or maintenance money did your corporation spend on security in the previous fiscal year?

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

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

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

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

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

? 21. Does your corporation allocate security resources based on facility criticality?

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

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

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IV. Corporate Security Program Management *continued*

YES NO

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

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

- National Fire Protection Association (NFPA)
- International Organization for Standardization (ISO)
- ASIS International
- American Petroleum Institute/National Petrochemical and 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. Are security incidents at your corporation managed centrally?

SENSITIVE SECURITY INFORMATION

SECTION IV. Corporate Security Program Management *continued*

❓ Corporate Security Program Management general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION V. 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?

? 2. | Does your corporation conduct criticality determinations at least every eighteen months?

? 3. | Does your corporation protect and limit access to criticality assessments and critical-facility lists?

4. Who has access to the list of critical facilities?

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

? 5. | Did you utilize the criteria from the 2011 TSA Pipeline Security Guidelines to determine your list of critical facilities?

6. | During the criticality assessment of your facilities, which of the following criteria were met?

- | | |
|--|---|
| Critical to national defense | National landmarks or monuments |
| Key infrastructure | Major rivers, lakes, or waterways |
| Mass casualty or significant health effects | Deliverability to significant number of customers |
| Disruption to state or local government public or emergency services | Business critical |

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION V. Risk Analysis — Security Vulnerability Assessment (SVA)

YES NO

? 7. Does your corporation conduct documented threat assessments?

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

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

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

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


? 10. Does your corporation conduct an SVA of your critical facilities periodically not to exceed 36 months?

SENSITIVE SECURITY INFORMATION


SECTION V. Risk Analysis — Security Vulnerability Assessment (SVA) *continued*


YES NO


- 11. When conducting an SVA, which of the following documented methodologies are you using?
Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER)
American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA)
Mission, Symbolism, History, Accessibility, Recognizability, Population, Proximity (MSHARPP)
Third-party or corporate proprietary
Other (if checked, elaborate in comment field)


-  12. Does your corporation conduct an SVA of your critical facilities after completing any significant enhancement or modification not exceeding twelve months?

-  13. Upon completion of an SVA, are corrective actions implemented within eighteen months?

-  14. Does your corporation conduct SVAs on your noncritical facilities?

-  15. Are facility support infrastructure such as water, electrical power, and telecommunications considered during the SVA?

-  16. Are the findings and recommendations from SVAs reviewed at the executive level?

-  17. Does your corporation protect and limit access to SVAs?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION V. Risk Analysis — Security Vulnerability Assessment (SVA) *continued*

18. Who in your corporation has access to completed SVAs?

- | | |
|----------------------------|--|
| Corporate management | Other facility managers |
| Security manager | All employees |
| Assistant security manager | Outside entity who assisted in the SVAs |
| Other security personnel | Other (if checked, elaborate in comment field) |
| Critical facility managers | |

 Risk Analysis general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VI. 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)

? 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 that could pose a security risk is not publicly available?

? 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?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VI. Operational Security *continued*

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

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



? Operational Security general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VII. Personnel and Contractor Security

YES NO

? 1. | Does your corporation conduct preemployment background checks on all your potential employees?

? 2. | Does your corporation conduct preemployment background checks based on the nature of the position?

3. | Which of the following types of preemployment background checks and screening does your corporation conduct?

- | | | |
|------------------------------------|-------------------------|---|
| Criminal | Employment verification | Alcohol/drug screening |
| Department of Motor Vehicles (DMV) | E-Verify | Other (if checked elaborate in comment field) |
| Credit | Education verification | |

? 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 persons with unescorted or unsupervised access to company critical facilities?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VII. Personnel and Contractor Security *continued*

YES NO

7. Which of the following persons have unescorted or unsupervised access to company critical facilities?

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

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

9. Which of the following are conducted during termination activities?

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

? **Personnel and Contractor Security general comments**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VIII. 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 | Patrols |
| Gates equivalent to attached barrier | Lighting |
| Signage such as No Trespassing, Do Not Enter, Authorized Personnel Only, CCTV in Use, etc. | Crime Prevention Through Environmental Design (CPTED) |
| Closed circuit television (CCTV) | Unarmed guards |
| Intrusion sensors | Armed guards |
| Alarms | Video-analytic systems |
| Clear zones around fence lines | Video recording |
| Locks | Intrusion-detection systems |
| Barriers such as bollards, planters, or Jersey barriers | Other (if checked, elaborate in comment field) |
| Tamper devices | |

3. Which of the following features are in use at your noncritical facilities?

- | | |
|--|---|
| Fences | Patrols |
| Gates equivalent to attached barrier | Lighting |
| Signage such as No Trespassing, Do Not Enter, Authorized Personnel Only, CCTV in Use, etc. | Crime Prevention Through Environmental Design (CPTED) |
| Closed circuit television (CCTV) | Unarmed guards |
| Intrusion sensors | Armed guards |
| Alarms | Video-analytic systems |
| Clear zones around fence lines | Video recording |
| Locks | Intrusion detection systems |
| Barriers such as bollards, planters, or Jersey barriers | Other (if checked, elaborate in comment field) |
| Tamper devices | |

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

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION VIII. Physical Asset Protection — Physical Security Measures *continued*

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**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IX. 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 | Security offices |
| Noncritical field facilities | Server rooms |
| Headquarters facility | Specific operational areas |
| SCADA Control Center | Other (If checked, elaborate in comment field) |

3. How does your corporation physically control normal access to controlled-access areas?

- | | |
|------------------|---|
| Lock and key | Proximity card |
| Biometric reader | Radio remote control |
| Digital keycard | Other (if checked elaborate in comment field) |

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

? 5. Do corporate personnel escort visitors while at controlled-access areas or critical facilities?

6. To whom does your corporation allow unescorted access to controlled-access areas?

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

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IX. Physical Asset Protection — Access *continued*

YES NO

? 7. | Does your corporation track, document, or digitally record access to controlled-access 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 | Contractors not assigned to the facility |
| Company employees assigned to the facility | Visitors |
| Company employees not assigned to the facility | Other (if checked, elaborate in comment field) |
| Contractors assigned to the facility | |

? 10. | Does your corporation ensure company or vendor identification is visibly displayed by employees and contractors while on-site?

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

? 12. | Does your corporation have a corporate key-control program?

? 13. | Does your corporation conduct a key inventory at least every 24 months?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION IX. Physical Asset Protection — Access *continued*

YES NO

? 14. | Does your corporation use patent keys to prevent unauthorized duplication?

? Physical Asset Protection — Access general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION X. 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 system(s)?

? 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 backup control center?

? 7. Does your corporation have a designated individual responsible for SCADA security?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION X. SCADA Security *continued*

YES NO

? 8. Do you restrict any remote operation of your SCADA system from portable electronic devices other than the pipeline control center?

? 9. Does your corporation perform a criticality assessment on your SCADA system(s) at least every eighteen months?

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

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

? 12. Is your corporation's SCADA system(s) housed on an isolated/segregated secure network?

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

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

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION X. SCADA Security *continued*

YES NO

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

- | | |
|--|--|
| Locked facilities | Access lists |
| Strong passwords | Entry logs |
| Communication gateways | Firewalls |
| Access-control lists | Demilitarized zone (DMZ) |
| Authenticators | Intrusion-detection system |
| Separation of duties | Intrusion-prevention system |
| Invocation of least privilege—only able to access information and resources that are necessary | Maintain patches |
| Keycards | Other (if checked, elaborate in comment field) |

? 16. Has your corporation developed a cross-functional cyber-security team for information security between your SCADA system(s) and enterprise networks?

17. Which of the following groups are represented on your corporate cyber-security team?

- | | |
|-------------------------------|---|
| Operations and/or maintenance | Third-party contractors or vendors |
| Information technology (IT) | Other (if checked elaborate in comment field) |

? 18. Has your corporation established security standards for evaluating the acquisition of SCADA-system devices and equipment?

? 19. Does your corporation only use SCADA workstations for approved control-system activities?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION X. SCADA Security *continued*

YES NO

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

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

? **SCADA Security general comments**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XI. Security Training

YES NO

? 1. | Does your corporation establish guidance for security training in your corporate security plan?

? 2. | Does your corporation require and conduct security-awareness training upon hire for all employees and contractors?

? 3. | Does your corporation require and conduct biennial refresher security-awareness training for all employees and contractors?

? 4. | Does your corporation require and conduct job-specific security training for all employees assigned security duties?

? 5. | Does your corporation require and conduct annual refresher job-specific security training for all employees assigned security duties?

? 6. | Does your corporation maintain security-related training records?

? 7. | Does your corporation conduct security orientations for visitors and vendors?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XI. Security Training *continued*

YES NO

? 8. | Does your corporation conduct SCADA-system(s) security training?

? 9. | Does your corporation conduct annual refresher training for SCADA-system(s) security?

? 10. To maintain security domain awareness, do your corporation's security personnel attend conferences, forums, or other advanced security training?

11. Have your corporation's security personnel availed themselves of any of the following training opportunities or affiliations?

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

? 12. Does your corporation use any of the TSA security-training material?

SECTION XI. Security Training *continued*

? Security Training general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XII. 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 | Security operations center |
| Noncritical facility | Maritime Transportation Security Act (MTSA) facility |
| SCADA center | Other (if checked elaborate in comment field) |
| Emergency operations center | |

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

- | | |
|---------------------------------------|---|
| Local emergency responders | Department of Homeland Security (DHS) |
| Tribal emergency responders | Transportation Security Administration (TSA) |
| State emergency responders | Neighboring corporations |
| Federal emergency responders | Other (if checked elaborate in comment field) |
| Federal Bureau of Investigation (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?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XII. Drill, Exercise, and Program Validation *continued*

YES NO

? 7. Does your corporation validate its security contact list periodically?

? 8. Does your corporation's security plan include a documented process for conducting periodic security audits of your facilities?

? **Drill, Exercise, and Program Validation general comments**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XIII. 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 use?

- | | |
|------------------------|------------|
| 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 test and evaluate communication equipment annually?

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

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XIII. Maintenance *continued*

 Maintenance general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XIV. Communications Devices and Mechanisms

YES NO

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

Email	Low band radio
Telephone	High band radio
Cellular telephone	Company band radio
Satellite telephone	Pager
Video conferencing	Other (if checked elaborate in comment box)

- ?** 2. Does your corporation have a mechanism, computer-driven process, or vendor services for automatic security notifications?

- ?** 3. Does your corporation use Government Emergency Telecommunications Service (GETS) cards?

? **Communications Devices and Mechanisms general comments**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XV. 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?

[Empty text box for question 1]

- 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)

[Empty text box for question 2]

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

- National Response Center (NRC), 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)

[Empty text box for question 3]

- 4. Does your corporation have an enterprise-wide system of security measures intended to be implemented based on credible threat information?

[Empty text box for question 4]

- 5. Does your corporation have site-specific security measures intended to be implemented based on credible threat information?

[Empty text box for question 5]

- 6. Are your corporation's site-specific security measures reviewed at least every eighteen months?

[Empty text box for question 6]

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XV. Security Incident Management *continued*

YES NO

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

[Empty text box for question 7]

8. 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 and/or maintenance
- Union representative
- Tenants
- Contractors
- Other (if checked, elaborate in the comment field)

[Empty text box for question 8]

9. From whom does your corporation receive current security threat information?

- Transportation Security Operations Center (TSOC)
- DHS Protective Security Advisor (DHS 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)

[Empty text box for question 9]

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

[Empty text box for question 10]

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

[Empty text box for question 11]

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XV. Security Incident Management *continued*

YES NO

? 12. Does your corporation have adequate staffing to implement security measures in response to security threat information?

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

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

? 15. During times of heightened alert, would your corporation limit physical access to noncritical facilities?

16. During times of Elevated 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 nonvital maintenance activities that could affect facility security

Delay or reschedule nonvital capital project work that could affect facility security

Increase lighting of facility buffer zones

Verify operating conditions of security systems— intrusion detection, cameras, or lighting

Request additional police patrols around the facility

Other (if checked, elaborate in the comment field)

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XV. Security Incident Management *continued*

17. | During times of Imminent Alert, would your corporation enact the following physical access controls at your critical facilities?

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

18. | During times of Elevated Alert, would your corporation enact any of the following measures on your SCADA system(s)?

- | | |
|---|--|
| Increase monitoring of intrusion-detection systems on your SCADA network? | Report any unusual SCADA-system network activity |
| Remind personnel to be vigilant regarding suspicious electronic mail | Other (if checked elaborate in comment field) |

19. | During times of Imminent Alert, would your corporation enact any of the following measures on your SCADA system(s)?

- 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)

SENSITIVE SECURITY INFORMATION

SECTION XV. Security Incident Management *continued*

YES NO

20. During times of Elevated Alert, would your corporation enact any of the following communication-related measures?

- | | |
|--|--|
| Inform all employees and on-site contractors of the increase or decrease to Elevated Alert | Liaison with local law enforcement to inform them of the change to Elevated Alert |
| Conduct security awareness briefings to all employees and on-site contractors | Liaison with local law enforcement to advise them of your Elevated Alert security measures |
| Brief employees and contractors on indicators of suspicious packages or mail | Verify operational capability of intelligence and emergency communications networks |
| Review response procedures for suspicious packages or mail | Monitor intelligence and emergency communications networks |
| | Other (if checked, elaborate in the comment field) |

[Empty comment box for question 20]

21. During times of Imminent Alert, would your corporation enact any of the following communication-related measures?

- | | |
|---|--|
| Inform all employees of the increase to Imminent Alert | Participate in scheduled situational briefings including TSA, local law enforcement, and industry associations |
| Conduct daily security and awareness briefings for each shift | Other (if checked elaborate in comment field) |

[Empty comment box for question 21]

22. Does your corporation utilize an incident-management system for security-related events?

[Empty comment box for question 22]

23. Does your corporation use the National Incident Management System (NIMS)?

[Empty comment box for question 23]

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

- | | | | |
|--|---------------------|---|--|
| Incident reporting | Arson | Terrorist attack | Insider threat |
| National Terrorism Advisory System (NTAS) levels | Riot | Active shooter | Hostage |
| Trespassing | Suspicious incident | Chemical, biological, radiological, or nuclear incident | Crime-scene management |
| Bomb threat | Crime or vandalism | | Other (if checked, elaborate in the comment field) |
| Pandemic | Surveillance | Cyber attack on SCADA system(s) | |

[Empty comment box for question 24]

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XV. Security Incident Management *continued*

YES NO

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

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

? 26. Does your corporation have a corporate emergency operations center for use during security incidents?

? **Security Incident Management general comments**

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XVI. 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

[Empty response box for question 1]

- 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)

[Empty response box for question 2]

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

[Empty response box for question 3]

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

[Empty response box for question 4]

- 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 Uninterrupted power source (UPS)/backup generators
Equipment for repair Other (if checked, elaborate in comment field)

[Empty response box for question 5]

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

[Empty response box for question 6]

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

SECTION XVI. Resilience *continued*

YES NO

? 7. Does your corporation have mutual aid agreements and/or alliances 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 such as breakout tanks, caverns, or LNG tanks to maintain the flow of product following a security-related event?

? 12. Is your pipeline system considered widely-dispersed as opposed to a long-haul pipeline with limited redundancy and resiliency?

? 13. Does your corporation have adequate financial reserves to redirect funds following a security-related event?

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVI. Resilience *continued*

? Resilience general comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVII. Final Comments

? Site or Control Center Visit Notes comments

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVII. Final Comments *continued*

 Recommendations

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVII. Final Comments *continued*

 Considerations

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

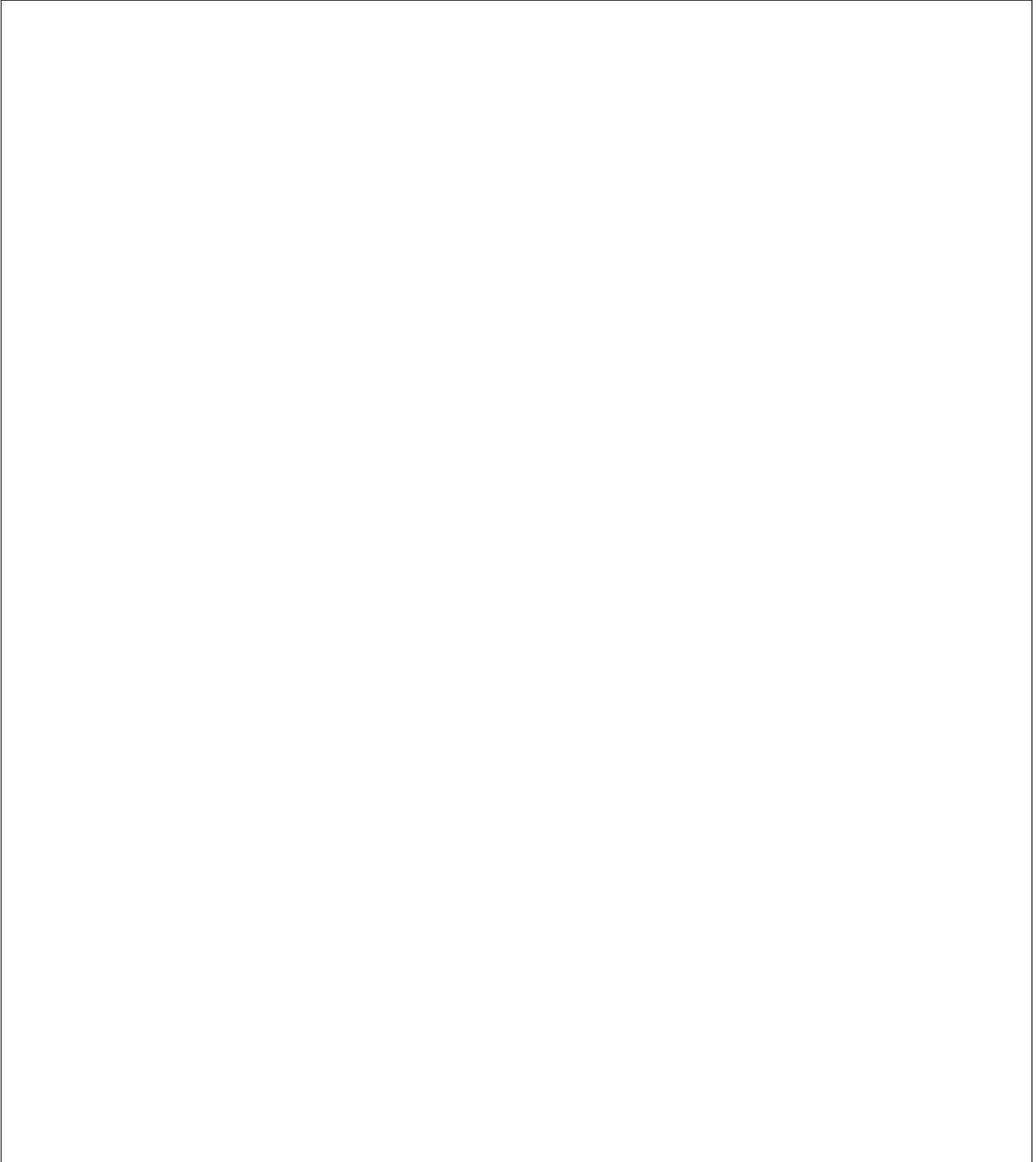
SECTION XVII. Final Comments *continued*

 Smart Practices

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVII. Final Comments *continued*

? Critical Facilities List



WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SECTION XVII. Final Comments *continued*

? References and Other Miscellaneous Notes

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

Visit Date: Report Date:

SECTION XVIII. Meeting Attendees

1. TSA Pipeline Security Division CSR Meeting Attendees

2. Pipeline Corporation CSR Meeting Attendees

3. Other CSR Meeting Attendees

4. CSR Form Filled Out by

--	--

WARNING: When filled in, this record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a need to know, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

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 response. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: TSA-11, Attention: PRA 1652-0056, 601 South 12th Street, Arlington, VA 20598.