|  |
| --- |
| DEPARTMENT OF HOMELAND SECURITYTransportation Security Administration**PIPELINE SECURITY****CRITICAL FACILITY SECURITY REVIEW (CFSR)** |
| **INSTRUCTIONS:** This form will be used by TSA personnel and their representatives to collect information on critical pipeline infrastructure during a Critical Facility Security Review. |
|  **SECTION I. Facility Information** |
|  | **Topic or Question** | **Answers** | **Comments** |
|   |  **General Facility Information** |
|  | Date of Review |  |  |
|  | Pipeline Company |  |  |
|  | Pipeline System |  |  |
|  | Pipeline Facility |  |  |
|  | Facility Street Address |  |  |
|  | City |  |  |
|  | State |  |  |
|  | County |  |  |
|  | Zip Code |   |  |
|  | Latitude (N) |  |  |
|  | Longitude (W) |  |  |
|  | Primary Corporate Security Point of Contact |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Office Phone |  |  |
|  | Mobile Phone |  |  |
|  | E-mail |  |  |
|  | Personnel Interviewed |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Office Phone |  |  |
|  | Mobile Phone |  |  |
|  | E-mail |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Office Phone |  |  |
|  | Mobile Phone |  |  |
|  | E-mail |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Office Phone |  |  |
|  | Mobile Phone |  |  |
|  | E-mail |  |  |
|  | TSA Review Team |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | Name |  |  |
|  | Title |  |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Observers (e.g., DOT, law enforcement, other operators) |  |  |
|  | Primary Commodity Category: | Crude OilRefined ProductsNatural Gas/LNGNGL/LPGToxic Inhalation Hazard (TIH) |  |
|  | Primary Facility Function(s):  | Gas Compressor StationLiquids Pump StationNatural Gas City Gate/Town Border StationPipeline InterconnectMeter/Regulator StationMainline Valve SiteBridge SpanNGL/LPG TerminalSecurity Operations CenterPipeline Control CenterBack-up Pipeline Control CenterMarketing TerminalUnderground Storage (note capacity)Above Ground Storage Tanks (note capacity)LNG Peak Shaving FacilityToxic Inhalation Hazard (TIH) FacilityOther (describe) |  |
|  | Is the facility staffed?  | NoYes |  |
|  | Staffing periods? | 24/77 days/week (days only)Monday-Friday, days and nightsMonday-Friday, days onlyMonday-Friday, partialN/AOther (describe)Varies with seasonUnknown |  |
|  | Total number of personnel who are present at the critical facility during day shifts? | 01-56-1516-2526-3536+N/AUnknown |  |
|  | Total number of personnel who are present at the critical facility during night/weekend/holiday shifts? | 01-56-1516-2526-3536+N/AUnknown |  |
|  | Is the facility a shared site with another pipeline operator, utility, or commercial entity? | NoYesUnknown |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Is the facility located within the perimeter of another company’s or operator’s facility?  | NoYesUnknown |  |
|  | Is the facility located within the secured perimeter of a military base? | NoYesUnknown |  |
|  | Is the facility regulated by the Maritime Transportation Security Act (MTSA)? | NoYesUnknown |  |
|  | Is all or part of the facility regulated by the Chemical Facility Anti-Terrorism Standards (CFATS)? | NoYesUnknown |  |
|  | Note general operational characteristics such as number and diameter of inbound/outbound pipelines, volumes of gas or liquids transported and/or stored, and acreage inside perimeter fencing. |  |
|  | Describe the most significant impact on downstream and upstream customers and interdependent infrastructure if the facility is inoperable. |  |
|  | **Risk Analysis and Assessments** |
|  | Which components are most vital to the facility’s continued operations? Select all that apply. | Electrical power infrastructure (substation, switchgear, etc.) Computer/data infrastructureManifold areaFacility control roomDehydration unitsPump motorsCompressor unitsWellheads (injection/withdrawal)Storage tanksRegulators/pressure controlOther (describe) |  |
|  | Are spare vital components available within 24 hours to support emergency restoration of service?  | NoUnknownYesPartialN/A |  |
|  | Estimated time to restore temporary/emergency service (i.e., minimally productive volumes) from a worst case scenario? | UnknownLess than one day1-5 days6-15 days16-30 days30 + days |  |
|  | Estimated reconstruction cost if facility is destroyed (in millions of dollars): | Unknown$0less than $10M$10M - $100M$100M - $500M$500M - $750MGreater than $750M |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Estimated daily loss of revenue if facility is temporarily inoperable: | UnknownLess than $50,000$50,000 - $100,000$100,000-$150,000$150,000- $200,000Greater than $200,000 |  |
|  | Based on the criteria presented in the TSA Pipeline Security Guidelines, why is the facility designated “critical?” Select all that apply.  | Criterion 1Criterion 2Criterion 3Criterion 4Criterion 5Criterion 6Criterion 7Criterion 8Other (describe) | See definitions in Section V. |
|  | Have security vulnerability assessments (SVA) been conducted at the facility? | NoUnknownYesPartial; not all SVA steps addressedPartial; not all pipeline assets addressedOther (describe) | See definitions in Section V. |
|  | Are SVAs conducted on an established schedule? | NoUnknownYes, every three years or more frequentlyYes, every four years Yes, every five years or less frequentlyN/A |  |
|  | Are appropriate findings implemented within 18 months of the completion of each SVA? | NoUnknownYesN/A |  |
|  | Have security audits been conducted at the facility? | NoUnknownYes, with internal non-security personnelYes, with internal security professionalsYes, with external government agenciesYes, with external security professionals Other (describe) | See definitions in Section V. |
|  | Are security audits conducted on an established schedule? | NoUnknownYes, annually or more frequentlyYes, every two yearsYes, every three years or less frequentlyN/A |  |
|  | **Site-Specific Measures** |
|  | Are security measures and procedures correlated to the DHS National Terrorism Advisory System (NTAS)? | NoUnknownYesN/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Have site-specific security measures and procedures been developed for the facility? | NoUnknownYesN/A  | See definitions in Section V. |
|  | Are site-specific security measures and procedures reviewed and updated as necessary on a periodic basis not to exceed 18 months? | NoUnknownYesN/A |  |
|  |  **Public Awareness** |
|  | Do the operator’s public awareness outreach efforts near this facility include security topics? | NoUnknownYesN/A |  |
|  | Which public awareness outreach efforts include security topics? Select all that apply. | Public awareness mailingsOperator’s corporate web siteLocal public meetingsDirect contact at residences and commercial facilities Other (describe)N/A |  |
|  | **Equipment Maintenance and Testing** |
|  | Are scheduled inspections of security measures conducted in order to detect damage, disrepair, tampering, etc.? | NoUnknownYesN/A | See definitions in Section V. |
|  | Does the operator have a maintenance program to ensure that the facility’s security equipment and systems are in good working order? | NoUnknownYesN/A |  |
|  | Does the operator verify the proper operation and/or condition of all security equipment on a quarterly basis? | NoUnknownYesPartial, not all security equipment and/or not on a quarterly basisN/A |  |
|  | Does the operator conduct annual inventories of security equipment? | NoUnknownYesN/A |  |
|  | Does the facility maintain alternate power sources (for example, generators or battery back-up) or equivalent equipment to minimize interruption of security equipment operation? | No, alternate power sources are not availableNo, alternate power sources are available but do not support security systemsUnknownPartialYesN/A, there are no electronic security systems at the facility |  |
|  | How often are alternate power sources tested? | Monthly or more frequentlyQuarterlyTwice per yearAnnually or less frequentlyNo established scheduleN/AUnknown |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | **Security Incident Response** |
|  | Note security incidents or suspicious activity at the facility in the previous five years. |  |
|  | Note names of nearby law enforcement agencies (LEA). |  |
|  | Has the facility maintained ongoing coordination/interaction with nearby law enforcement agencies on security topics? | NoUnknownYesN/A |  |
|  | How often does the facility coordinate/interact with nearby law enforcement agencies on security topics? | Annually or more frequentlyEvery 2-3 yearsEvery 4-5 yearsEvery six years or less frequentlyUnknownN/A |  |
|  | Has the facility maintained ongoing coordination/interaction with neighboring pipeline facilities, refineries, and similar facilities on security topics such as coordinated responses to various threat conditions? | NoUnknownYesN/A |  |
|  | Are emergency contact lists printed and/or readily accessible to facility employees? | NoUnknownYesN/A |  |
|  | Are bomb threat response checklists printed and readily accessible near facility telephones? |  NoUnknownYesN/A |  |
|  | **Personnel Identification and Badging** |
|  | Are photo identification badges issued to company employees who are assigned to the facility? | NoUnknownYesN/A |  |
|  | Which of the following groups are issued identification badges when at the facility? Select all that apply. | NoneCompany employees not assigned to the facilityLong-term, trusted contractorsOther contractorsTransient visitors (UPS, FedEx, waste disposal, etc.)Others (describe)UnknownN/A |  |
|  | Which of the following groups are required to display identification badges when at the facility? Select all that apply. | NoneCompany employees assigned to the facilityCompany employees not assigned to the facilityLong-term, trusted contractorsOther contractorsTransient visitors (UPS, FedEx, waste disposal, etc.)Others (describe)UnknownN/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | **Access Control Procedures** |
|  | Are any contractors given the same access privileges as employees? | NoUnknownYesN/A |  |
|  | What steps are taken to authenticate those without authorized access? Select all that apply. | NoneVerbal screeningVisual screeningID check at access control pointScheduled appointmentsVerification with visitor’s employerOther (describe)Unknown |  |
|  | Which of the following groups are required to sign a facility log that documents the date/time/purpose of their visit? Select all that apply. | NoneCompany employees assigned to the facilityCompany employees not assigned to the facilityLong-term, trusted contractorsOther contractorsTransient visitors (UPS, FedEx, waste disposal, etc.)Others (describe)UnknownN/A |  |
|  | Which of the following groups are escorted or monitored while at the facility? Select all that apply. | NoneCompany employees not assigned to the facilityLong-term, trusted contractorsOther contractorsTransient visitors (UPS, FedEx, waste disposal, etc.)Others (describe)UnknownN/A |  |
|  |  **Personnel Training** |
|  | Do facility employees receive initial security awareness training in either a computer-based or classroom format? | No UnknownYes, classroomYes, computer-basedYes, both formatsOther (describe)N/A |  |
|  | Does the security awareness training include information from TSA developed training materials? | NoUnknownYesN/A |  |
|  | Do facility personnel receive periodic refresher training on security awareness topics? | NoUnknownYes, classroomYes, computer-basedYes, both formatsOther (describe)N/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | What is the frequency of refresher training? | Annually or more frequentlyEvery 1-2 yearsEvery three years or less frequentlyN/AUnknown |  |
|  | Does the operator maintain security training records? | NoUnknownYesN/A |  |
|  | **Exercises and Drills** |
|  | Do facility personnel conduct or participate in periodic security drills or exercises? | NoUnknownYesN/A |  |
|  | How often do facility personnel conduct or participate in security drills or exercises?  | N/AUnknownAnnually or more frequentlyEvery two yearsEvery three years or less frequentlyNot on an established scheduleOther (describe) |  |
|  | Does the operator develop and implement a written post-exercise report assessing security exercises and documenting corrective actions? | NoUnknownYesN/A |  |
|  | Does the operator invite representatives from law enforcement agencies to participate in security drills and exercises? | NoUnknownYes, representatives invited but did not attendYes, representatives invited and attended N/A |  |
|  |  **Guard Force** |
|  | Are security personnel deployed at the facility during baseline threat conditions? For example, is a guard posted at the main gate to support access control and monitoring? | NoUnknownYes, but not 24/7Yes, 24/7 |  |
|  | Describe security personnel. Select all that apply. | Company employeesContractors (Securitas, Wackenhut, etc.)Off-duty law enforcement personnelOther (describe)UnknownN/A |  |
|  | What percentage of security personnel carry a firearm? | 0%1-25%26-50%51-75%75+%N/AUnknown |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Does the operator or facility maintain a contract with a commercial guard company that ensures rapid availability of security personnel in a crisis? | NoUnknownYesN/A |  |
|  |  **Information Protection** |
|  | Are printed copies of sensitive security documents protected from unauthorized access?  | NoUnknownYesN/A |  |
|  |  **Barriers – Perimeter Fencing** |
|  | Is perimeter fencing installed at the facility? | NoUnknownYesN/A |  |
|  | Select the type(s) of perimeter fencing material(s). Select all that apply. | Chain-linkWoodCinder block or brickSheet metalNo-climb meshCombination of aboveOther (describe)N/A |  |
|  | Is a barbed wire or razor wire topper installed on perimeter fencing? | NoUnknownYesPartialN/A |  |
|  | What type of barbed wire and/or razor wire is installed on perimeter fencing? Select all that apply. | Outward facing barbed wireInward facing barbed wireY-shaped barbed wireVertical barbed wireRazor wireOther (describe)N/A |  |
|  | Including the barbed wire or razor wire topper, what is the approximate overall height of perimeter fencing (as measured when standing on the outside of the fence)? If fencing varies in height, select the height of the shortest section. | under 5-feet6-feet7-feet8-feetover 8-feetN/A |  |
|  | Does perimeter fencing fully enclose the facility’s vital components? | NoUnknownYesN/A |  |
|  | Are two layers of fencing installed around the facility’s vital component(s)? | NoUnknownYesN/A |  |
|  | Is there a clear zone of several feet on either side of the fence that is free of obstructions, vegetation, or objects that could be used by an intruder to scale the fence?  | NoUnknownYesN/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Does vegetation growth degrade the security effectiveness of the perimeter fence? | NoUnknownYesN/A |  |
|  | Does damage or disrepair degrade the security effectiveness of the perimeter fence?  | NoUnknownYesN/A |  |
|  | Does erosion, drainage areas, or gaps under the fence degrade the security effectiveness of the perimeter fence? | NoUnknownYesN/A |  |
|  |  **Barriers - Perimeter Gates** |
|  | How many perimeter vehicle gates are motorized? | 012-34-67+N/AUnknown |  |
|  | Do personnel monitor motorized gates until they close? | NoUnknownYesOther (describe)N/A |  |
|  | Do large gaps between gate panels and/or posts degrade the security effectiveness of the barrier? Select all that apply. | NoYes, pedestrian gate(s)Yes, emergency egress gate(s)Yes, manual vehicle gate(s)Yes, motorized vehicle gate(s)N/A |  |
|  | Does erosion, drainage areas, or gaps under gates degrade the security effectiveness of the barrier? Select all that apply. | NoYes, pedestrian gate(s)Yes, emergency egress gate(s)Yes, manual vehicle gate(s)Yes, motorized vehicle gate(s)N/A |  |
|  | Does damaged or substandard barbed wire or razor wire on perimeter gates degrade the security effectiveness of the barriers? Select all that apply. | NoYes, pedestrian gate(s)Yes, emergency egress gate(s)Yes, manual vehicle gate(s)Yes, motorized vehicle gate(s)N/A |  |
|  | Can emergency egress gates be manipulated and opened from outside the fence?  | NoUnknownYesN/A |  |
|  | Are all perimeter gates secured when not in active use? | NoUnknownYesN/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Which groups have keys to padlocks on perimeter gates? Select all that apply.  | Company employeesLong-term, trusted contractorsOther contractorsPipeline operators or utilities that share the siteTransient visitors (UPS, FedEx, waste disposal, etc.)Emergency respondersOthers (describe)UnknownKey distribution is not trackedN/A |  |
|  | Are padlocks from other entities daisy-chained with company padlocks on perimeter gates? | NoUnknownYesN/A |  |
|  | Are keys to padlocks on perimeter gates stamped "Do Not Duplicate" or does the facility utilize restricted key blanks to prevent or deter unauthorized duplication? | NoUnknownYesN/A |  |
|  | Are key control procedures established and documented for key tracking, issuance, collection, and loss? | NoUnknownYesN/A |  |
|  | Are periodic key inventories conducted? | NoYes, annually or more frequentlyYes, every 24 monthsYes every 36 months or less frequentlyYes, but not on an established scheduleN/AUnknown |  |
|  |  **Barriers - Vehicle Barriers** |
|  | Are vehicle barriers installed on the facility’s perimeter, near access control points, and/or near vital components?  | NoUnknownYesNo, but barriers are stored on-site and can be rapidly deployed N/A |  |
|  | Select all types of installed vehicle barriers. | Jersey barriersBollardsNatural barriers (ditch, large rocks, trees)Guard railsHeavy equipmentSteel cableOther (describe)N/A |  |
|  | Are barriers crash-rated per the standards of the U.S. Department of State? | NoYes, K-12Yes, K-8Yes, K-4N/AUnknown |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | **Electronic Access Controls** |
|  | Are electronic access control systems installed at the facility?  | NoUnknownYesN/A |  |
|  | Which groups have authorized access to perimeter gates that utilize electronic access controls? Select all that apply. | Company employees not assigned to the facilityLong-term, trusted contractorsOther contractorsPipeline operators or utilities that share the siteTransient visitors (UPS, FedEx, waste disposal, etc.)Emergency respondersOthers (describe)UnknownN/A |  |
|  | Which access points are controlled by the electronic access control system? Select all that apply. | Perimeter vehicle gatesInterior vehicle gatesPedestrian gatesExterior doors to facility buildingsInterior doors at facility buildings that lead to sensitive areasOther (describe)N/AUnknown |  |
|  | Select the type(s) of authentication required by the system(s). Select all that apply. | Proximity card readerKeypad/PIN CodeWireless/remote gate opener Physical keyBiometricOther (describe)N/AUnknown |  |
|  | Does the system log access by authorized personnel? | NoUnknownYesN/A |  |
|  | Does the system record access attempts by unauthorized personnel? | NoUnknownYesN/A |  |
|  | Does the system alert employees to access attempts by unauthorized personnel? | NoUnknownYesN/A |  |
|  | Are access control records periodically audited to ensure compliance with policies and procedures? | NoUnknownYesN/A |  |
|  | **Intrusion Detection and Monitoring – Video Camera System** |
|  | Is a CCTV system installed at the facility? | NoUnknownYesN/A |  |
|  | Is the CCTV system fully functional? | NoUnknownYesN/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | How many total cameras are installed? | 12-34-67+N/AUnknown |  |
|  | How many of the installed cameras offer pan-tilt-zoom (PTZ) capability? | 12-34-67+N/AUnknown |  |
|  | Where are video images displayed? | At the facilityRemotely at pipeline control centerRemotely at a security control centerRemotely at a third party monitoring serviceRemotely at another Company facility At other location (describe)Not displayedN/AUnknown |  |
|  | Is the system designed and managed in a manner that provides a 24/7 capability to detect and assess unauthorized access? | NoUnknownYesN/A |  |
|  | To support incident response, can real-time video feeds be monitored off-site by those with valid log-in credentials? | NoUnknownYesN/A |  |
|  | Does the CCTV system enable personnel to screen visitors prior to granting entry? | NoUnknownYesN/A |  |
|  | Does the CCTV system monitor or record activity around vital components? | NoUnknownYesN/A |  |
|  | Select all enhanced capabilities of the camera system.  | Motion-activated alertsMotion-activated recordingVideo analyticsIR illuminationOther (describe)NoneN/AUnknown |  |
|  | Where are video images recorded? Select all that apply. | Not recordedUnknown At the facilityOff-site pipeline controlOff-site security control center Other location (describe)N/A |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | How many days of video imagery are stored before they are deleted or recorded over? | 0Unknown 1-1415-3031-4545-6061+N/A |  |
|  | Did the review team review image quality from the CCTV cameras? | NoYes, imagery was generally excellentYes, imagery was acceptableYes, imagery was generally poorN/A |  |
|  | **Intrusion Detection and Monitoring - Intrusion Detection System (IDS)** |
|  | Is an intrusion detection system (IDS) installed at the facility? | NoUnknownYesN/A |  |
|  | Is the IDS fully functional? | NoUnknownYesN/A |  |
|  | Is the system designed and managed in a manner that provides a 24/7 capability to detect and assess unauthorized access? | NoUnknownYesN/A |  |
|  | What types of sensors are installed and operational? Select all that apply. | Microwave Magnetic contactsPassive infrared (PIR)Fence disturbance sensorsMechanical switchesOther (describe)N/AUnknown |  |
|  | Does a siren, horn, or similar device broadcast IDS alarms across the facility in a manner that alerts personnel of a potential security event? | NoUnknownYesN/A |  |
|  | Does the frequency of false or nuisance alarms impact the effectiveness of the IDS system? | NoUnknownYesN/A |  |
|  |  **Facility Lighting** |
|  | Is exterior lighting installed at the facility? | NoUnknownYesN/A |  |
|  | How is the lighting activated? Select all that apply. | photo cell sensorstimermanualmotionother (describe)N/A Unknown |  |
|  | **Topic or Question** | **Answers** | **Comments** |
|  | Are primary access control points adequately illuminated? | NoUnknownYesPartialN/A |  |
|  | Are vital components adequately illuminated? | NoUnknownYesPartialN/A |  |
|  | Does the lighting provide adequate illumination for the CCTV cameras (if installed)? | NoUnknownYesPartialN/A |  |
|  |  **Security Signage** |
|  | Are “No Trespassing,” “Authorized Personnel Only,” or signs of similar meaning posted along the perimeter fence? | NoYes, in a manner that is visible from all approaches Partial, only at access control pointsPartial, not in a manner that is visible from all approachesOther (describe)N/AUnknown |  |
|  | If a CCTV system is installed, are signs posted warning that the premises are under video surveillance? | NoUnknownYesN/A |  |

**SECTION II. Comments**

**SECTION III. Recommendations**

**SECTION IV. Aerial Photograph**

**SECTION V. Definitions**

|  |
| --- |
| **Criteria for Critical Facilities**According to the TSA Pipeline Security Guidelines, pipeline facilities meeting one or more of the criteria below are considered to be critical: A facility or combination of facilities that, if damaged or destroyed, would have the potential to: 1. Disrupt or significantly reduce required service or deliverability to installations identified as critical to national defense;
2. Disrupt or significantly reduce required service or deliverability to key infrastructure (such as power plants or major airports) resulting in major economic disruption;
3. Cause mass casualties or significant health effects;
4. Disrupt or significantly reduce required service or deliverability resulting in a state or local government’s inability to provide essential public services and emergency response for an extended period of time;
5. Significantly damage or destroy national landmarks or monuments;
6. Disrupt or significantly reduce the intended usage of major rivers, lakes, or waterways. (For example, public drinking water for large populations or disruption of major commerce or public transportation routes);
7. Disrupt or significantly reduce required service or deliverability to a significant number of customers or individuals for an extended period of time;
8. Significantly disrupt pipeline system operations for an extended period of time (i.e., business critical facilities).

**Security Vulnerability Assessments (SVA)**A security vulnerability assessment (SVA) is one of the risk assessment methodologies pipeline operators may choose. The SVA serves as a planning and decision support tool to assist security managers with identifying, evaluating, and prioritizing risks; and determining effective security measures to mitigate threats and vulnerabilities to their critical facilities. Common steps performed while conducting an SVA include: 1. Asset Characterization - identification of hazards and consequences of concern for the facility, its surroundings, and its supporting infrastructure; and identification of existing layers of protection;
2. Threats Assessment - description of possible internal and external threats;
3. Security Vulnerability Analysis - identification of potential security vulnerabilities, existing security measures, and their level of effectiveness in reducing identified vulnerabilities;
4. Risk Assessment - determination of the relative degree of risk to the facility in terms of the expected effect on each asset and the likelihood of a success of an attack; and
5. Security Measures Analysis - strategies that reduce the probability of a successful attack or reduce the possible degree of success, strategies that enhance the degree of risk reduction, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

**Security Audits**A security audit is a structured assessment of the operator’s implementation of security policies and procedures at a specific facility. Audits typically include interviews with facility personnel, reviews of security-related documents and records, and a facility inspection. **Site-Specific Measures**Operators should develop, document, and implement site-specific security measures for each of their critical facilities. These measures should be tailored explicitly for each individual facility, with emphasis on specific procedures and actions to be taken at different threat levels. On a periodic basis, not to exceed 18 months, these facility specific measures should be reviewed and updated as necessary.**Security Inspections**Security inspections are the examination of physical and electronic security measures to ensure that they are delivering the designed security benefit to the facility. Additionally, security inspections should document signs of disrepair or damage to security measures, vandalism or theft of property, and indications of criminal, terrorist, or suspicious activity. |

**Paperwork Reduction Act Statement:**

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. Transportation Security Administration estimates that the average burden for collection is 4 hours.  You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to:  TSA-11, Attention: PRA 1652-0050 601 South 12th Street, Arlington, VA 20598