Pipeline Security Smart Practice Observations

September 19, 2011

Transportation
Security
Administration

Transportation Security Administration

September 2011

Pipeline Security Smart Practice Observations

The Transportation Security Administration (TSA) *Pipeline Security Smart Practice Observations* is a tool for pipeline security professionals seeking concepts or ideas to improve their security program. This document is a compilation of the smart security practices that were observed by the TSA Pipeline Security Division during Corporate Security Reviews (CSRs) and Critical Facility Inspections (CFIs) of pipeline companies.

These *Pipeline Security Smart Practice Observations* are an update of those first released by TSA in 2006. The earlier pipeline security smart practices were observed between the 2003 initiation of the CSR program and 2006. The CSR program was initiated to reduce risk and deter acts of terrorism that exploit pipeline infrastructure. As of mid-2011, CSRs have been conducted on 100% of the top 100 pipeline systems in the country that collectively transport 84% of all hazardous liquid and natural gas. TSA began reevaluating the top 100 systems in the fall of 2008. Reevaluating systems enables TSA to assess a pipeline operator’s current security programs in comparison to their programs from previous years.

Since 2006, TSA has observed many additional pipeline security smart practices and wishes to share them among all pipeline stakeholders through this newly released TSA *Pipeline Security Smart Practice Observations* document. These observations come, in part, from the CFI Program, developed in 2008 and consistent with requirements of the *Implementing Recommendations of the 9/11 Commission Act of 2007*. By mid-2011, 347 critical facilities from the top 100 pipeline systems in the country have been inspected.

For user-convenience, the TSA *Pipeline Security Smart Practice Observations* have been sorted into primary and secondary security categories. In the Microsoft® Excel version, the user can search smart security practice observations by category, search the document using the filter tool, or use a simple word search. In the Adobe® version, the user can search the smart security practice observations using the word-search feature.

The TSA Pipeline Security Division hopes all users of the TSA *Pipeline Security Smart Practice Observations* will find new and innovative solutions to their security challenges based on both those pipeline security smart practices currently used in the industry and new ones developed by encompassing the foundational work of their industry peers.

Transportation Security Administration

September 2011

Pipeline Security Division

Pipeline Security Smart Practice Observations

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Corporate Security Plan		**Procedures for release of security documents**—Developed a company procedure to control release of sensitive or security-related documents. The company security director or manager provided written approval prior to the distribution, copying, forwarding, or releasing of any part of the company security plan.
Corporate Security Plan		**Security plan change management**—Documented and implemented a change-management process for revisions to the security plan. • Conducted reviews and updates of the security plans periodically and on an as-needed basis. • Maintained a revision history of all changes and dates. • Developed and utilized an approval section in the security plan that includes a dated signature from a responsible management representative.
Corporate Security Plan		**Threat information receipt and dissemination**—Established company procedures to ensure timely delivery of critical threat information to appropriate persons in the company. Established company procedures to alert outside agencies of specific threats.
Corporate Security Plan		**Transmitting threat information to employees**—Formalized a process for screening and transmitting pertinent threat information to employees. Processes included automated communication mechanisms, company intranet, and computer-driven communication systems.
Corporate Security Plan		**Work-management systems**—Utilized an electronic work-management system to track security action items.
Corporate Security Plan		**Guard-force guidance**—Established communications, recordkeeping, standard operating procedures, and post orders for guard personnel.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Corporate Security Program		**Audit findings**—Provided a summary of frequent security items found during audits, site visits, and security checks to company managers. Worked in conjunction with management to prioritize and resolve identified problems.
Corporate Security Program		**Audit program**—Combined the review of the company security plan with existing internal audit program(s).
Corporate Security Program		**Benchmarking**—Benchmarked security efforts with other companies and industries. Shared best security practices and lessons learned for continuous improvement
Corporate Security Program		**Bomb-threat management program**—Created a bomb-threat management program that • Provides training for employees • Prevents or deters a bomb from entering a critical site • Provides early detection • Provides appropriate response measures • Includes facility design that mitigates damages • Details response procedures following an explosion
Corporate Security Program		**Defined roles and responsibilities**—Developed a security plan based on a security risk-management process that clearly defines roles and responsibilities for the development, implementation, control, review, continual improvement, and approval of the security program across the organization.
Corporate Security Program		**Executive accountability**—Ensured corporate management is knowledgeable and accountable for oversight and adherence to the security program and plan.
Corporate Security Program		**Formal security committee**—Developed a security committee or team to actively guide and manage the security program. Representatives from security, operations, regulatory compliance, information technology, engineering, health, environment and safety, human resources, legal, and executive leadership were considered for membership.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Corporate Security Program		**Law enforcement agency/security liaisons**—Created a position within the company for a law enforcement/intelligence sharing liaison to act as an intermediary between law enforcement agencies and security organizations within the company and industry as a whole.
Corporate Security Program		**Security clearance**—Ensured company employees responsible for enterprise-level security functions hold a Secret clearance so that, in the event of an emergency or other security situation, they can receive classified government information regarding their company.
Corporate Security Program		**Security funding**—Established a dedicated budgetary allowance for routine security expenditures and projects.
Corporate Security Program		**Security plan access**—Maintained a signed non-disclosure agreement (NDA) on file for any person who accesses the security plan. Redacted versions, where sensitive materials are removed from the security plan, may be shared with all employees or posted to the company's intranet or other communication media.
Corporate Security Program		**Security practices sharing**—Shared security practices among peer companies for benchmarking opportunities to optimize each company's security-program management; ensured reference to company name and identity were removed.
Corporate Security Program		**Security professionals**—Incorporated third-party security professionals when a situation requires additional expertise or in-depth security knowledge.
Corporate Security Program		**Strong management structure focused on security**—Ensured security considerations are integrated into core elements of the company's management guidance documents.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Cyber Security Measures	**General Cyber Security Measures**	**Access control**—Provided an access-control system to ensure only authorized persons have access to controlled spaces. For control centers, limited access with authentication devices such as smart or magnetic identity keycards and/or biometric readers. Utilized camera systems to monitor entrances to control centers.
Cyber Security Measures	**General Cyber Security Measures**	**Alternate control center**—Provided an offsite alternate control center that can maintain control of the pipeline system if the primary control center is damaged or becomes uninhabitable.
Cyber Security Measures	**General Cyber Security Measures**	**Biometric authentication**—Installed biometric devices that authenticate approved employee access to control centers.
Cyber Security Measures	**General Cyber Security Measures**	**Change Management**—Provided a configuration or change-management policy and procedure to ensure approved or proper modifications or alterations to hardware, firmware, or software for the SCADA system.
Cyber Security Measures	**General Cyber Security Measures**	**Control and communication cabling**—Protected and secured cable runs to limit ease of access by installing within solid conduits, locked cabinets, direct burial, or other appropriate means.
Cyber Security Measures	**General Cyber Security Measures**	**Control-system personnel hiring policies**—Conducted preemployment screening such as background checks and in-depth interviews to screen candidates that will have control or maintenance access to control systems. Developed detailed job descriptions describing duties with terms and conditions of employment.
Cyber Security Measures	**General Cyber Security Measures**	**Cross-functional security team**—Created a cross-functional team that, at a minimum, includes company personnel responsible for cyber security and those responsible for physical security. Developed a partnership to address security risks in both the cyber and physical environments.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Cyber Security Measures	**General Cyber Security Measures**	**Duress alarms—**Installed hidden duress alarms in control centers in the event there is unauthorized intrusion.
Cyber Security Measures	**General Cyber Security Measures**	**Employment termination—**Revoked physical and electronic access to SCADA systems immediately following the termination, relocation, or reassignment of any employee with control-center access.
Cyber Security Measures	**General Cyber Security Measures**	**Hot-swapping—**Installed equipment and software with the ability to swap control to an alternate control center at the touch of a button.
Cyber Security Measures	**General Cyber Security Measures**	**Keycard access to work computers**—Required keycard access to all work-issued laptop and desktop computers, utilizing keycards employing smart-card technology. Users must place a micro-chipped ID card into a computer slot and subsequently enter separate passwords for computer, network, and email access.
Cyber Security Measures	**General Cyber Security Measures**	**Media protection—**Secured portable media such as CDs, DVDs, USB memory sticks, portable and hard drives. Trained personnel on the proper use, transport, storage, and disposal of the media. Disabled auto-start features in the computer operating system so that media is not allowed to automatically play. Monitored for unauthorized connections of mobile devices to control-system interfaces.
Cyber Security Measures	**General Cyber Security Measures**	**Obscurity—**Removed any signage or other discernable identifier that indicates the presence of a SCADA system or pipeline control center.
Cyber Security Measures	**General Cyber Security Measures**	**Password protection—**Instituted individual-user password requirements on all interactions with SCADA control systems. Two-factor authentication such as a password and keycard was incorporated at critical facilities.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Cyber Security Measures	**General Cyber Security Measures**	**Physical segregation of SCADA from other systems**—Physically segregated/separated/air-gapped control networks from enterprise system networks, company intranet, and the Internet. Disallowed use of any nonessential or unauthorized software, games, Internet, or email through control-system networks.
Cyber Security Measures	**General Cyber Security Measures**	**Portable computers**—Secured and protected any portable computer that is used on the SCADA system. When portable computers were used, then restricted the remote SCADA access to specific computers and specific users. SCADA-system portable computers are not connected to the Internet and unapproved software is prohibited.
Cyber Security Measures	**General Cyber Security Measures**	**Protect SCADA field devices**—Physically secured SCADA field devices—such as remote terminal units and communications devices—with locks and further installed an intrusion-detection system (IDS) that communicates with the control center in the event of tampering.
Cyber Security Measures	**General Cyber Security Measures**	**Protection of SCADA physical assets**—Provided a defense-in-depth layered physical security approach to securing SCADA control centers, buildings, facilities, rooms, equipment, and any other important SCADA assets. Utilized physical barriers, fencing, barricades, intrusion detection, closed-circuit television, and/or other measures as appropriate.
Cyber Security Measures	**General Cyber Security Measures**	**Removal, disposal, or destruction of equipment**—Implemented a policy and procedure(s) to address the removal, disposal, or destruction of control-system equipment.
Cyber Security Measures	**General Cyber Security Measures**	**SCADA backup power systems**—Provided backup power to SCADA systems and equipment with an uninterruptible power supply (UPS) through alternate power source(s), battery, or standby generator systems.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Cyber Security Measures	General Cyber Security Measures	**SCADA fail-safe processes**—Set all SCADA-actuated operations devices to limit transients or damage, or fail-safe in the event of lost SCADA control or lost communications.
Cyber Security Measures	General Cyber Security Measures	**SCADA security-response procedures**—Prepared plans and procedures for pipeline control-center personnel who receive incoming calls regarding suspicious events or other security-related events along the pipeline system.
Cyber Security Measures	General Cyber Security Measures	**SCADA-specific program and plan**—Documented and instituted a SCADA-specific security program and plan that encompasses not only cyber aspects but also physical-security aspects that protect SCADA components and human-interface points.
Cyber Security Measures	General Cyber Security Measures	**SCADA-specific vulnerability assessments**—Conducted a SCADA-specific physical-security vulnerability assessment for the SCADA system and its physical components. Evaluated ease of access and physical security measures instituted to protect the control center and field devices. In addition, identified and evaluated all SCADA communication lines or network connections that could be tapped or exploited.
Cyber Security Measures	General Cyber Security Measures	**Security-awareness training for SCADA controllers**—Provided security-awareness training for SCADA controllers. In addition, provided training to field operations personnel so they understood the importance of security on SCADA physical assets in the field. Training covered both control system-specific issues and physical security measures required to protect SCADA assets in the field.
Cyber Security Measures	General Cyber Security Measures	**Separation of control-system duties and least privilege**—Instituted a pipeline control-center policy where access to resources and privileges was limited to those necessary for employees to perform their job function.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Cyber Security Measures	General Cyber Security Measures	**Visitors—**Prohibited access to control centers for any guests, vendors, nonessential employees, or any other individual who does not have a need-to-know or approved functional purpose.
Cyber Security Measures	General Cyber Security Measures	**Wireless access—**Avoided all wireless networking in SCADA systems.
Cyber Security Measures	Information Security Coordination and Responsibilities	**Document security**—Protected sensitive information by shredding documents when no longer needed, locked file cabinets and trash bins, instituted a clean-desk policy, and marked sensitive documents as Confidential or Sensitive Security Information (SSI).
Cyber Security Measures	Information Security Coordination and Responsibilities	**Internet postings**—Screened all company-posted information that appears on the Internet. Evaluated information to be posted for security-sensitive information such as detailed maps, photos, and documents that could be utilized by an adversary to build an attack plan.
Cyber Security Measures	Information Security Coordination and Responsibilities	**Laptop-theft tracking**—Used a software program to track stolen laptops. The software theft-recovery company works with local law enforcement to return the laptop to the proper owner.
Cyber Security Measures	System Restoration and Recovery	**Redundant SCADA systems**—Utilized duplicate SCADA systems to provide an immediate backup in the event of a failure.
Facility Security Measures	Communication	**Affiliate corporate relationships**—Maintained working relationships and partnerships with corporate- or global-security departments when they are housed in different business entities than pipeline security operations.
Facility Security Measures	Communication	**Affiliate security department relationships**—Developed working relationships with security departments of companies where a joint-venture or other business relationship between pipelines or affiliate companies exists.

Pipeline Security Smart Practice Observations

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	Communication	**Automated notification system**—Utilized a dedicated automated incident-management communication system that automatically notifies key personnel in the event of an incident or threat. Common modes of communications that can be programmed into the automated system can include landlines, cell phones, satellite phones, email, and text messages.
Facility Security Measures	Communication	**Bomb-threat checklists**—Ensured bomb-threat checklists are printed and readily available near facility telephones.
Facility Security Measures	Communication	**Community crime-prevention program**—Partnered with local community programs such as Crime Stoppers and Neighborhood Watch to raise security awareness and increase reporting of suspicious incidents.
Facility Security Measures	Communication	**Community involvement**—Distributed a periodic landowner-awareness letter to adjacent property owners, encouraging the reporting of suspicious incidents.
Facility Security Measures	Communication	**Compensation for landowners who monitor unmanned facilities**—Compensated landowners near unmanned facilities for their assistance in monitoring facilities and reporting suspicious activity to a 24-hour emergency contact number.
Facility Security Measures	Communication	**Coordination with first responders through an appreciation event**—Hosted an appreciation event at pipeline facilities to show appreciation and bolster relations with local law enforcement and other first responders.
Facility Security Measures	Communication	**Coordination with local law enforcement**—Improved coordination with local law enforcement agencies by providing tours, exchanging contact information, and highlighting the facility(s)' critical role in the region's energy infrastructure.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Communication**	**Government Emergency Telecommunications Service (GETS)**—Provided key company executives and security personnel GETS cards to use in the event of an emergency or crisis situation where the landline and cellular telephone network is overloaded.
Facility Security Measures	**Communication**	**In-case-of-emergency contact card**—Issued an in-case-of-emergency telephone contact card to company personnel. The card has the phone numbers of the company Security Control Center, SCADA Control Center, and other pertinent company contacts. Issued laminated pocket cards with emergency contact information for both company personnel and off-site responders.
Facility Security Measures	**Communication**	**Incident reporting**—Established anonymous employee hotlines to encourage employees to report suspicions.
Facility Security Measures	**Communication**	**Interaction with industry**—Participated in pipeline-industry security working groups such as Interstate Natural Gas Association of America (INGAA), American Gas Association (AGA), Association of Oil Pipelines (AOPL), American Public Gas Association (APGA), and American Petroleum Institute (API) as appropriate.
Facility Security Measures	**Communication**	**Internal collaboration**—Ensured interdepartmental relationships and information-sharing is a priority at every level of the company. In addition, allowed security staff to provide security-related information and advice to all business units or departments when advisable.
Facility Security Measures	**Communication**	**LEPC membership**—Participated in local emergency planning committees (LEPC) or regional security coordination committees.
Facility Security Measures	**Communication**	**Local law enforcement speed dial**—Installed a direct-dial phone line between the company control room and local law enforcement.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	Communication	**Multilingual security pamphlet/signage**—Created multilingual security pamphlets and signage if operating in an area where languages other than English are commonly spoken.
Facility Security Measures	Communication	**Public outreach and community assistance**—Established strong working relationships with local first responders including law enforcement, fire departments, and EMS/EMT services.
Facility Security Measures	Communication	**Public security awareness materials**—Distributed low-cost items such as refrigerator magnets, pens, notepads, and calculators displaying company security-contact information to ensure that adjacent landowners know what number to call to report suspicious activity on or near the pipeline.
Facility Security Measures	Communication	**Reward program**—Created a community-watch reward program for the reporting of suspicious activity that warrants further investigation by the company or law enforcement personnel.
Facility Security Measures	Communication	**Security awareness component in mailed materials**—Included a security component in the company's public awareness mailings.
Facility Security Measures	Communication	**Security coordination with neighboring companies**—Improved security coordination with neighboring companies to ensure that security incidents are shared and lessons collectively learned. Met regularly with adjacent entities to share security information and, if possible, coordinated security efforts. Discussed resource availability and establish mutual-aid agreements.
Facility Security Measures	Communication	**Tenant–landlord relationships**—Coordinated closely with building management or lessees on security topics such as response procedures for heightened threat conditions.
Facility Security Measures	Communication	**Ties with federal law enforcement**—Familiarized the company with various federal law enforcement agencies and their locally focused mission.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	Design and Construction	**Conduits, wires and cables**—Buried or otherwise protected conduits and wires carrying electrical supply, telecommunications, and alarm signals.
Facility Security Measures	Design and Construction	**Emergency and normal power distribution**—During the design phase of construction, segregated normal and emergency power systems including power sources, load centers, and distribution infrastructure.
Facility Security Measures	Design and Construction	**Emergency generator protection**—Ensured emergency generators installed outdoors at grade are protected by perimeter walls and locked entrances. Areas prone to flooding were avoided. Allowances for ease of access to refueling locations and fuel-line shutoff valves, and also proximity of generator(s) to the building were incorporated.
Facility Security Measures	Design and Construction	**Incorporation of security into major construction projects**—Incorporated security considerations into major construction projects; as an example, established a separate contractor entrance and posted a guard at construction entrances for increased access control.
Facility Security Measures	Design and Construction	**Laminated security glass**—Installed laminated security glass or bullet-resistive glazing in appropriate locations such as pipeline or gas control centers and SCADA server rooms.
Facility Security Measures	Design and Construction	**Physical security standards**—Developed and utilized a standard that establishes a consistent framework for the design, installation, and operating requirements of physical security protection, surveillance, and monitoring devices for the protection of employees, company assets, information, and intellectual property.
Facility Security Measures	Design and Construction	**Vaults**—Buried critical components in underground vaults and protected the entry doors with intrusion-detection systems (IDS).

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	Drills and Exercises	**Collaboration with other stakeholder drills and exercises**—Participated in drills and exercises sponsored by other local stakeholders and adjacent businesses.
Facility Security Measures	Drills and Exercises	**Exercises and drills**—Evaluated the strengths and weaknesses of all security plans through the use of annual security drills that test a specific component of a security plan and through the use of exercises that test multiple components or functions to include interaction with outside entities.
Facility Security Measures	Drills and Exercises	**Facility penetration tests**—Conducted random unannounced or covert facility penetration tests of all access points around a given facility. Ensured fences are properly maintained and monitored.
Facility Security Measures	Drills and Exercises	**Guard force participation in drills and exercises**—Required guards to participate in company exercises, drills, and tabletop exercises.
Facility Security Measures	Drills and Exercises	**Internal auditing mechanisms**—Utilized a security-compliance spreadsheet and auditing checklist combined with education and coaching on standards interpretation, during an actual walk-around-assessment. Included a gap analysis and committed to a specific timeline to address identified issues.
Facility Security Measures	Drills and Exercises	**Internal security monitoring**—Incorporated security reviews and audits into the company's existing Environment, Health, and Safety (EHS) Audit Program.
Facility Security Measures	Drills and Exercises	**Lessons learned**—Utilized security incidents as training opportunities to capture lessons learned, test incident response and reporting, and underscore the need for continued vigilance and security awareness.
Facility Security Measures	Drills and Exercises	**Local law enforcement**—Conducted live and tabletop exercise operations with regional law enforcement agencies, producing unity of effort through common training and coordinated prevention and response capabilities.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Drills and Exercises**	**National Energy Security Professionals (NESP)**—Attended National Energy Security Professionals (NESP) meetings.
Facility Security Measures	**Drills and Exercises**	**National Level Exercise (NLE)**—Participated in a Department of Homeland Security (DHS) National Level Exercise (NLE) and other federal, state, or local exercises.
Facility Security Measures	**Drills and Exercises**	**Safety drills and exercises**—Added a security component to safety drills and exercises. From these drills, company security advisors established follow-up tasks to improve both the safety and the security at their facilities.
Facility Security Measures	**Drills and Exercises**	**Security audits**—Conducted security audits on an established schedule not to exceed 12 months.
Facility Security Measures	**Drills and Exercises**	**Seminars for emergency responders**—Hosted seminars for local law enforcement, fire departments, and emergency managers to familiarize them with the company's critical facilities and its security and emergency response programs.
Facility Security Measures	**Drills and Exercises**	**Tabletop exercises**—Conducted tabletop exercises twice a year incorporating all pertinent employees. When an employee was absent during the tabletop, they were required to attend a similar tabletop at another facility or area office.
Facility Security Measures	**Drills and Exercises**	**Templates**—Posted drill templates, scenarios, examples, and evaluations on the company intranet to aid field managers.
Facility Security Measures	**Equipment Maintenance and Testing**	**Backup power supply testing**—Tested backup power sources on an established schedule to ensure working order.
Facility Security Measures	**Equipment Maintenance and Testing**	**Backup SCADA testing**—Established and tested the backup SCADA controls, equipment, and communication devices on a periodic basis. Verified and load-tested backup power sources for all servers, network components, and vital workstations.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	Equipment Maintenance and Testing	**CCTV and IDS tests and inspections**—Ensured that tests and inspections of the CCTV and IDS systems are conducted per the maintenance inspection form and/or manufacturers' recommendations.
Facility Security Measures	Equipment Maintenance and Testing	**Communication testing**—Maintained a regular test schedule for all company communication devices, networks, and systems.
Facility Security Measures	Equipment Maintenance and Testing	**Equipment inspection checklist**—Created an inspection checklist for security equipment.
Facility Security Measures	Equipment Maintenance and Testing	**General maintenance**—Provided appropriate inspection and general maintenance of all facilities and assets. Conducted repairs as necessary to lighting, fencing, gates, doors, locks, and windows.
Facility Security Measures	Equipment Maintenance and Testing	**Good housekeeping**—Maintained good housekeeping at all facilities to avoid the impression that lack of care equals lack of security.
Facility Security Measures	Equipment Maintenance and Testing	**Monitoring reliability testing**—Conducted annual reliability tests of intrusion-detection and CCTV-monitoring systems.
Facility Security Measures	Equipment Maintenance and Testing	**Perimeter fence and gate inspection and repair**—Performed ongoing fence and gate inspection and maintenance. This included removing fallen branches and clearing vegetation from the fence line, repairing erosion, and maintaining clear zones.
Facility Security Measures	Equipment Maintenance and Testing	**Work-management tracking system**—Utilized computer work-management tracking systems to program maintenance and testing activities for security devices.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Personnel Training**	**CCTV, IDS, and digital video recorder (DVR) training**—Ensured employees are well trained in utilizing the CCTV system and IDS to detect and investigate suspicious activity. Operators are trained how to use the on-site DVR for reviewing captured images and recorded alarms.
Facility Security Measures	**Personnel Training**	**Education**—Attended security conferences, training sessions, and participated in trade association security committees in order to stay knowledgeable of new security technologies and trends.
Facility Security Measures	**Personnel Training**	**Guard force skills**—Hired guards trained in a variety of screening techniques, system security operations, and knowledgeable in the tactics used to avoid detection.
Facility Security Measures	**Personnel Training**	**Intranet security training portal**—Created an interactive intranet-based training program for security-related topics.
Facility Security Measures	**Personnel Training**	**Periodic security updates**—Distributed security updates company-wide to keep employees informed of security events and trends.
Facility Security Measures	**Personnel Training**	**Recognition of violent tendencies**—Taught employees how to recognize the early warning signs of a troubled or potentially violent person and how to respond.
Facility Security Measures	**Personnel Training**	**Security and periodic safety meetings**—Integrated security component(s) into monthly safety and tailgate meetings providing a frequent opportunity to discuss security-related issues, events, and essential security information. Initial and refresher security training classes, however, were reserved for dedicated training sessions.
Facility Security Measures	**Personnel Training**	**Security brochure and orientation**—Provided all visitors and contractors entering the property a security brochure and orientation that includes information on restricted items, restricted areas, security responsibility, dangerous substances and devices, and security sensitive information.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Personnel Training**	**Security posters**—Displayed security posters, pamphlets, stickers, or other media that remind visitors and employees to remain vigilant, to report suspicious items and behavior, and to remember the various methods of reporting suspicious activity.
Facility Security Measures	**Personnel Training**	**Security reporting criteria**—Trained employees to identify what unusual or suspicious activities or security-related events should be reported and educated employees regarding the reporting process. This criteria included suspicious activity and descriptions of what happened, where and when it happened, how many people were involved, and how and to whom to report the information.
Facility Security Measures	**Personnel Training**	**Security training and Operator Qualifications (OQ)**—Included security-training mandates in operator qualification requirements.
Facility Security Measures	**Personnel Training**	**Security training program**—Developed and implemented a security training program that includes security-awareness training for new employees, refresher training for current employees, and security-focused drills and exercises. Provided security topics such as roles and responsibilities, security-related procedures for all threat conditions, detection, and response to suspicious personnel and items. Emphasized that all employees in an organization must understand security policies and procedures exist, there is a good reason for why they exist, they must be enforced, and there are serious consequences for infractions. Provided refresher training on an established schedule.
Facility Security Measures	**Personnel Training**	**Specialized training for local first responders**—Trained local first responders on the intricacies of the facility and general security-awareness concepts.
Facility Security Measures	**Personnel Training**	**Suspicious items**—Trained company employees and contractors on detecting and responding to suspicious items.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Personnel Training**	**Tanker driver security training**—Provided security-awareness training for drivers who enter company properties such as marketing terminals or crude trucking facilities. Training included procedures for reporting suspicious activities.
Facility Security Measures	**Personnel Training**	**Training record database**—Maintained training records in an electronic database that has the ability to generate training reports.
Facility Security Measures	**Personnel Training**	**Train-the-trainer sessions**—Provided security topic train-the-trainer (TTT) sessions for presenters. The TTT sessions are conducted by security professionals.
Facility Security Measures	**Personnel Training**	**TSA audio-visual training aids**—Enhanced security training through use and presentation of TSA Pipeline Security Division training CDs, DVDs, and other available materials.
Facility Security Measures	**Security Incident Procedures**	**Alternate operations center for security response**—Established an off-site alternate operations center for security-incident response coordination. Stocked the alternate operations site with adequate supplies including telephones, computers, faxes, radios, system maps, standard operating procedures (SOPs), table, chairs, basic office supplies and other basic provisions.
Facility Security Measures	**Security Incident Procedures**	**Crisis communication plan**—Created a crisis-communication plan that details communication procedures, capabilities, and resources and contains a telephone list of various groups to be contacted in a security emergency to include the incident management team, utility personnel, mutual-aid partners, media contacts, and affected landowners surrounding a site.
Facility Security Measures	**Security Incident Procedures**	**Guard force company-specific emergency response awareness**—Trained guards on company emergency-preparedness plans and company response resources.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Security Incident Procedures**	**Incident Command System (ICS)**—Utilized the Incident Command System during security incident response. Practiced security incident response with the ICS teams.
Facility Security Measures	**Security Incident Procedures**	**Incident-response procedures**—Provided all pipeline employees and contractors with security-incident response procedures including what to do in the event of bomb threats, pipeline system or asset destruction, unauthorized entry, workplace violence, SCADA or IT attacks, health and safety emergency, or an environmental contamination threat.
Facility Security Measures	**Security Incident Procedures**	**Memorandum of Understanding (MOU)**—Established an MOU, cooperative agreement, or mutual-aid agreement with local, regional, state, and federal agencies as well as other pipeline companies and partners to provide cascading of resources that fill critical gaps during security events or emergencies.
Facility Security Measures	**Security Incident Procedures**	**National Threat Advisory System (NTAS) postings**—Posted security alert levels and definitions for employees through convenient methods such as the company intranet and/or clearly visible postings.
Facility Security Measures	**Security Incident Procedures**	**Notification expectations and lists**—Defined notification policies and ensured those policies were understood by all employees and contractors. Identified appropriate federal, state, and local agencies to contact upon a suspected terrorist incident.
Facility Security Measures	**Security Incident Procedures**	**Off-site command post for critical facilities**—Arranged an off-site incident command post for each critical facility. Used this command post if normal facility access was lost during a security incident or exercise. Locations used included neighboring businesses, motel conference or banquet rooms, and warehouses.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures	**Security Incident Procedures**	**Security investigations**—Created and utilized a security investigation process that included the use of trained professionals and incorporated strong interaction with law enforcement and government security agencies.
Facility Security Measures	**Security Incident Procedures**	**Security team threat level response**—Followed the National Threat Advisory System (NTAS) and tied the frequency of the company's security team meetings to the operating company threat level; as an example, for no NTAS threat level, the team meets monthly. For a threat level of Elevated, the team meets weekly. For a threat level of Imminent, the team meets daily.
Facility Security Measures		**Avoided single facility access and egress**—Provided alternative facility access and egress routes; minimized facility access and egress points during routine operations; and provided multiple access and egress capability adding flexibility in the event a primary path is lost. Exercised using alternate facility access and egress points periodically.
Facility Security Measures		**Backup power for security systems**—Provided backup power sources for security equipment such as access control, lighting, gate controls, CCTV, alarms, and related computer systems. Backup power sources can include uninterruptible power supply (UPS) units, emergency electrical generators, and protected distribution systems from reliable sources.
Facility Security Measures		**Binoculars**—Provided facility staff or guard forces with powerful binoculars that can be used for surveillance of the property and for emergencies. The binoculars allowed up-close viewing from a safe distance. A spotting-scope was used at a large facility because it worked better in low-light situations.
Facility Security Measures		**Contract Resources**—Maintained contracts with companies capable of quickly repairing the pipeline or facilities in the event of pipeline damage.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Facility Security Measures		**Pipeline system redundancy**—Maintained sufficient operational redundancy in the pipeline system so that an attack against the company is less likely to cause significant impact to company operations and the regional or national pipeline infrastructure.
Facility Security Measures		**Piping and fittings for emergency use**—Maintained a supply of pretested company-owned pipe and fittings to use during an emergency repair. Maintained the list and the list's contents at centrally located regional or district offices.
Facility Security Measures		**Security representation**—Designated an on-site employee to serve as a responsible party and security representative at critical facilities, in a pipeline-operations region, or in a specific business unit.
Facility Security Measures		**Site-specific security plan**—Developed site-specific security plans that identify baseline and enhanced security measures to be applied during heightened threat levels. This includes general post orders for the deployment of security personnel and equipment. Prepared written copies of the site-specific security plan and made them readily accessible, especially in the event of a power or network failure.
Facility Security Measures		**Strategic alliance with suppliers**—Maintained strategic alliances with key suppliers and other similar companies through reciprocal agreements to facilitate rapid restoration of damaged critical facilities.
Personnel Security	Background Investigation	**Background checks**—Ensured all company employees are subject to background checks regardless of their employment status as part-time, full-time, or contractor. Differentiated between categories of background checks based on area of employment, placing higher emphasis on the more sensitive positions or responsibilities.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Personnel Security	**Background Investigation**	**Background screening tiers**—Conducted employee background screening on three progressive levels—basic, management, and executive.
Personnel Security	**Background Investigation**	**Criminal-history checks**—Used criminal background checks to assess the suitability of employees for positions. Utilized the federally established list of disqualifying crimes applicable to hazmat drivers and transportation workers at ports—see 49 CFR 1572.103—for unmonitored access to company-designated critical infrastructure.
Personnel Security	**Background Investigation**	**Periodic criminal history screening**—Periodically reviewed employee criminal history.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Personnel Security	Background Investigation	**Redress policy—**Established a vigorous internal redress process for adversely affected applicants and personnel that includes an appeal and waiver process similar to the system established for hazmat drivers and transportation workers at ports—see 49 CFR Part 1515. • Designed an appeal process to provide an applicant or personnel with the opportunity to show he or she does not have a disqualifying conviction by correcting outdated underlying court records or proving mistaken identity. • Designed a waiver process to provide an applicant or personnel with the opportunity to be hired or continue employment by demonstrating rehabilitation or facts surrounding a conviction that mitigate security concerns. The process permits an applicant or personnel to submit information pertaining to any of the following: • Circumstances of the disqualifying offense • Restitution made • Letters of reference from clergy, employers, probation/parole officers • Other factors the individual believes bear on his or her good character The redress process was incorporated into disciplinary procedures already in use as part of management/labor relations.
Personnel Security	Background Investigation	**Social Security Number verification**—Used the Social Security Number Verification System (SSNVS) that the Social Security Administration (SSA) makes available to all employers to verify that current employee names and social security numbers match SSA records.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Personnel Security	**Background Investigation**	**Verification of immigration status**—Used the E-Verify program to determine employee eligibility after hire. Submitted information taken from a new hire's Form I-9, Employment Eligibility Verification, through E-Verify to the Social Security Administration and U.S. Citizenship and Immigration Services (USCIS) to determine whether the information matches government records and whether the new hire is authorized to work in the United States.
Physical Security and Access Controls	**Access Controls**	**Access-badge encoding**—Encoded all issued badges with the appropriate level of access necessary for an employer or contractor to perform job duties.
Physical Security and Access Controls	**Access Controls**	**Access-log review**—Periodically reviewed access logs to ensure only authorized persons are entering the facility.
Physical Security and Access Controls	**Access Controls**	**Anti-passback access control**—Used anti-passback software to prevent employees from giving their cards or PIN numbers to someone else to use, thus preventing more than one entry at a time for a given card.
Physical Security and Access Controls	**Access Controls**	**Auditable key-management and access-media program**—Implemented a key issuance, tracking, and return system for key and access media. When an employee no longer required access, all keys and access media were recovered or disabled. When keys or access media were reported lost or stolen, they were deactivated and/or locks were changed. Access media included cardkeys, electronic keys, biometric devices, and remote gate openers.
Physical Security and Access Controls	**Access Controls**	**Audits of proximity cards**—Periodically audited the lists of persons issued proximity cards for access control to ensure that only persons with a current need are allowed access to sensitive areas.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	**Access Controls**	**Biometric data and photo incorporated into access card**—Combined a photo and biometric data into one card allowing for both visual identification, confirmation, and remote access-control that can be logged electronically. Card color varies with employment status; as an example, employee cards are blue, contractor cards are red, and visitor cards are green.
Physical Security and Access Controls	**Access Controls**	**Biometrics: hand/palm scanner**—Implemented a hand/palm scanner system for access. The hand/palm scanner verifies the user and prevents unauthorized use of an employee's access card. The employee swipes or presents a proximity card, then has their palm scanned for entry.
Physical Security and Access Controls	**Access Controls**	**Building-entry point control**—Ensured all building entry points to critical areas are controlled and/or monitored. Reduced the number of building entry points, particularly under periods of heightened threat, thereby lowering vulnerability and security costs associated with monitoring and controlling access.
Physical Security and Access Controls	**Access Controls**	**Challenge IDs**—Ensured ID badges were issued to all employees. Trained employees to challenge persons who are not wearing badges.
Physical Security and Access Controls	**Access Controls**	**Comprehensive access-control and badging system at company headquarters**—Installed access-keycard readers outside all office entrance doors and conference rooms, the company lobby, and in stairwells on floors where operations are located. The card readers record the employee or contractor name and identification number assigned to their badge, the date, and time of use. Records are stored in a database and retained for up to one year after deactivation of the card.
Physical Security and Access Controls	**Access Controls**	**Control of facility parking**—Ensured access to facility parking is limited, where possible, to company vehicles and personnel. At a minimum, authorized parking spaces and vehicles are registered and identified.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	Access Controls	**Control-room access alarms**—Established the capability for control-room personnel to monitor access alarms on the doors leading to the control room and company server rooms.
Physical Security and Access Controls	Access Controls	**Control-room and critical-component hardening**—Secured, hardened, and reinforced entrances leading to company control rooms. Hardened the control room and other critical components by using blast doors, laminated walls, and multi-paned bullet-proof/blast-resistant glass.
Physical Security and Access Controls	Access Controls	**Control-room entry restriction—**Revised access-control lists so that contractor or vendor personnel are not able to gain unescorted access to pipeline control-room spaces.
Physical Security and Access Controls	Access Controls	**Control-room entry screening**—Incorporated methods that allow control-room personnel to visually screen visitors prior to granting entry.
Physical Security and Access Controls	Access Controls	**Covert-entry routes**—Ensured facilities cannot be accessed by nontraditional means such as loading docks, poles, ladders, skylights, or below-grade windows and doors.
Physical Security and Access Controls	Access Controls	**Displaying identification badges**—Required employees, contractors, and visitors to wear company-issued ID badges at all times. Displayed individual's name and current photo on issued access-control cards.
Physical Security and Access Controls	Access Controls	**Electronic visitor-management system**—Incorporated an electronic or computer-based visitor management system and badging process to reduce human error.
Physical Security and Access Controls	Access Controls	**Enhanced window protection**—Hardened standard windows with metal grates or glass laminate, replaced standard windows with glass-clad polycarbonate, or laminated polycarbonate blast-resistant windows to mitigate blast damage.
Physical Security and Access Controls	Access Controls	**Foot traffic**—Installed personnel gates and turnstiles for foot traffic entering a facility.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	**Access Controls**	**Front-desk intercom**—Installed an intercom system at the front desk to screen visitors before entry to secure areas of the building.
Physical Security and Access Controls	**Access Controls**	**ID verification**—Performed inspections of employee and visitor identification.
Physical Security and Access Controls	**Access Controls**	**Key duplication**—Used patent keys to prevent unauthorized duplication of company keys.
Physical Security and Access Controls	**Access Controls**	**Personal Identification Numbers (PIN)**—If access controls utilize a programmable personal identification number (PIN), required the PIN to contain eight or more alpha-numeric characters and instituted a scheduled PIN-change timeframe.
Physical Security and Access Controls	**Access Controls**	**Preapproval for visitors**—Required visitors to undergo a background check in advance of their visit to critical facilities.
Physical Security and Access Controls	**Access Controls**	**Remote location access-control**—Used security-card access systems at remote locations such as compressor stations or pump stations. Each division or business unit determined access levels to their respective facilities.
Physical Security and Access Controls	**Access Controls**	**Tailgate sensors**—Used tailgate sensors at access-control points to ensure that only one authorized person at a time is granted access. The sensor alarms when more than one person per access card passes.
Physical Security and Access Controls	**Access Controls**	**Unauthorized parking**—Established and implemented parking procedures to include signage notifying the public about towing policies and the removal of unauthorized vehicles.
Physical Security and Access Controls	**Access Controls**	**Vehicle screening area**—Provided adequate lighting in screening area to illuminate the vehicle exterior and undercarriage. When conducting vehicle screening, at a minimum, included a visual inspection of the vehicle exterior, undercarriage, passenger compartment, and trunk. Provided CCTV coverage of the screening process. For higher risk facilities, more thorough inspections are used.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	**Access Controls**	**Vehicle-access point reduction**—Reduced the number of vehicle access points, particularly under periods of heightened threat. This reduces vulnerability and security costs associated with monitoring and controlling access to the site.
Physical Security and Access Controls	**Access Controls**	**Vehicular guardhouse communications**—Placed a telephone or intercom in all active vehicular guardhouses.
Physical Security and Access Controls	**Access Controls**	**Visitor colored-access badges**—Distributed distinctively colored badges encoded with restricted-access controls to visitors.
Physical Security and Access Controls	**Access Controls**	**Visitor digital color photo ID cards**—Used digital color photo on ID card to allow for verification of visitor.
Physical Security and Access Controls	**Access Controls**	**Visitor electronically-timed access-control badges**—Used an electronically-timed access badge for visitors. The badge is embedded with a smart chip that allows the visitor access only to specific areas. The smart chip is programmed with a timed expiration code that denies the visitor facility access beyond the prescribed time.
Physical Security and Access Controls	**Access Controls**	**Visitor escort requirements**—Established visitor escort requirements; as an example, personnel escorting visitors must maintain a visual line of sight, physical proximity, or other means of control of the visitor(s). • Established the ratio of visitors to escorts. • Vetted visitors prior to granting access to confirm their identity and security clearances as needed. • Required approval for unescorted access based on company policy.
Physical Security and Access Controls	**Access Controls**	**Visitor escorts**—Escorted all contractors and visitors to include employee guests, vendors, and others who may require access, especially when visiting critical facilities.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	**Access Controls**	**Visitor screening**—Checked identification and maintained a log of site visitors. If visitor is a vendor or contractor, called their employer to verify/validate their identification.
Physical Security and Access Controls	**Access Controls**	**Visitor's Center**—Established a Visitor's Center, located on the exterior of the facility's perimeter fence, for check-in and screening.
Physical Security and Access Controls	**Barriers**	**Adjacent-facility security measures**—Networked with adjacent companies who share the same fence line, thereby benefitting from their security measures.
Physical Security and Access Controls	**Barriers**	**Bottom support rail for chain-link fence**—Provided a bottom wire or bar on fence sections to make it more difficult to lift the fence from the bottom.
Physical Security and Access Controls	**Barriers**	**Clear view into a facility**—Avoided use of fencing, landscaping, or walls that might block visibility into a facility and provide hiding places along the perimeter.
Physical Security and Access Controls	**Barriers**	**Clear zones**—Created clear zones extending six feet or more from facility perimeters that are free of tall shrubs, trees, and any stored items that could be used as climbing aids.
Physical Security and Access Controls	**Barriers**	**Daily security inspection**—Conducted a perimeter fence walk each day to detect and address signs of intrusion.
Physical Security and Access Controls	**Barriers**	**Enhanced vehicle barriers**—Included physical barriers inside the perimeter to ensure drivers keep to intended areas and maintain distance from critical components.
Physical Security and Access Controls	**Barriers**	**Fence height plus outriggers**—Ensured that the effective height of the entire perimeter fence is seven feet or higher with three strands of barbed or razor wire mounted on outriggers. Extended the outriggers outward at a 45-degree angle to deter persons from attempting to climb over it.
Physical Security and Access Controls	**Barriers**	**Fencing, vegetation growth, and erosion**—Addressed vegetation growing over or near fence lines as well as areas of erosion beneath the fence fabric.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	Barriers	**K-rated vehicle barriers**—Used K-rated vehicle barriers at the main gate of critical facilities.
Physical Security and Access Controls	Barriers	**Line-of-sight**—Maintained a clear line-of-sight along and adjacent to perimeter fencing, critical assets, and buildings. Maintained shrubbery less than three to four feet tall and kept trees pruned up to at least seven to eight feet from the ground.
Physical Security and Access Controls	Barriers	**Multiple fences**—Added an internal fence line that surrounds the facility's critical components, particularly at large facilities. Installed additional line of security fencing a minimum of 10 to 20 feet. inside the perimeter fence to create a controlled area for sensors or perimeter patrols between fences. Use of additional fencing slows persons breaching the perimeter.
Physical Security and Access Controls	Barriers	**Pipeline infrastructure**—Used sturdy fences or panels to protect infrastructure such as pipes, valves, meters, and other appurtenances that could be tampered with or damaged.
Physical Security and Access Controls	Barriers	**Signage phone number(s)**—Ensured perimeter fencing signs contain phone number to call if unusual or suspicious activity is observed.
Physical Security and Access Controls	Barriers	**Spare material for perimeter protection**—Used items such as spare/used pipes and river weights to supplement and harden existing perimeter barriers.
Physical Security and Access Controls	Barriers	**Vehicle access to facility perimeter**—Designed site vehicle routes to prevent high-speed approaches to critical areas. Used barriers or offset facility access points from the direction of a vehicle's approach to force a reduction in speed.
Physical Security and Access Controls	Barriers	**Vehicle barrier staging**—Staged portable vehicle barriers near gate entries to ease deployment during heightened threat conditions.
Physical Security and Access Controls	Barriers	**Vehicle barriers around perimeter fence**—Placed vehicle barriers such as Jersey barriers, ditches, and boulders around facilities or installed fencing cables.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	Barriers	**Vehicle entrance barriers**—Utilized critical-facility entrance barriers that resist vehicular ramming such as pop-up bollards, hydraulic ramps, wedges, and plate barriers.
Physical Security and Access Controls	Facility Lighting	**Adequate lighting for parking areas**—Verified parking-area lighting effectively provides for employee safety and deters illegal or threatening activities.
Physical Security and Access Controls	Facility Lighting	**CCTV night capability**—Assessed CCTV image quality at night and determined if new cameras and/or upgraded lighting is needed.
Physical Security and Access Controls	Facility Lighting	**Facility-entrance lighting**—Designed company entrances to be well-lit, well-defined, and highly visible to the public and pipeline employees. Verified lighting near the main gate enhances the ability of operators to screen visitors via CCTV.
Physical Security and Access Controls	Facility Lighting	**Lighting survey**—Conducted a lighting survey to ensure critical components can be adequately monitored 24/7.
Physical Security and Access Controls	Facility Lighting	**Motion-activated lighting for critical components**—Installed motion-activated lighting to minimize the facility profile.
Physical Security and Access Controls	Facility Lighting	**Perimeter lighting**—Increased perimeter lighting especially during heightened threat levels.
Physical Security and Access Controls	Gates	**Facility-specific padlocks**—Used unique padlocks or combination locks on facility perimeter gates and to secure critical components within the perimeter of a facility.
Physical Security and Access Controls	Gates	**Multiple padlocks**—Removed excess and/or unknown padlocks from perimeter gates. Did not authorize others to daisy-chain padlocks on critical facilities or components without permission.
Physical Security and Access Controls	Gates	**Unattended perimeter gates**—Kept all perimeter gates securely padlocked after-hours and when not in use.
Physical Security and Access Controls	Gates	**Unused perimeter gates**—Secured unused gates with a Jersey barrier, heavy chains and locks, or some other means to prevent unauthorized access.

Pipeline Security Smart Practice Observations

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Access-road detection**—Installed IDS systems along facility-access roads that alert company to approaching vehicles.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Audible and visual alarms**—Used audible and visual intrusion-detection alarms at all company-designated critical facilities and, when possible, all unmanned and remote facilities.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Backup power for security alarms and monitoring systems**—Provided, at a minimum, a four-hour battery backup or alternate power source to all security alarm and monitoring systems.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV 24-hour surveillance advisory**—Installed warning signs advising of 24-hour CCTV/video surveillance at entrances to any site, facility, parking garage, and anywhere CCTV coverage exists to deter potential criminals.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV and IDS alarm receipt**—Ensured alarms generated by the CCTV system and IDS are brought to operators' attention both audibly and visually.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV blind spots**—Designed CCTV camera coverage so that there are no blind spots.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV data transmission**—Verified CCTV data is transmitted on an IT LAN and determined if the LAN has the capability of providing the minimum level of video resolution, frame rate, and system reliability to satisfy physical-security protection needs.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV installation strategy**—Installed CCTV cameras in a strategy that supports visual screening of personnel at perimeter vehicle gates.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV monitor size**—Installed an on-site high-resolution video monitor large enough to clearly display CCTV views.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV monitoring**—Ensured intrusion-detection alarms and CCTV systems are monitored at computer workstations in an operator’s security or SCADA control center, and used third-party security-monitoring services in some instances.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV motion detection**—Used CCTV with motion-detection and video-analytic capabilities at all company-designated critical facilities and, when possible, at unmanned and remote facilities 24-hours per day.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV-system permanent wiring**—Installed permanent power supplies for the CCTV system. Avoided temporary wiring and use of extension cords.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**CCTV-video and security-alarm data storage**—Stored digital security system alarms and CCTV system images for at least 30 days.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Door and window alarms**—Installed alarms on doors and windows that provide access to critical areas so that any unauthorized entry will alert appropriate alarm-monitoring personnel.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Fence-motion sensors**—Installed perimeter fence IDS-disturbance wiring or fence-shake sensors at critical facilities.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Integrated video analytics**—Integrated perimeter IDS with CCTV systems to monitor or record alarms reported by the IDS system.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Motion-detection technology**—Installed motion-detection technology at access control points and near critical components that alert operators to movement.
Physical Security and Access Controls	Intrusion Detection and Monitoring	**Remote-site CCTV**—Installed IP-addressable cameras and intrusion-detection systems at all remote facilities and critical components such as compressor stations or pump stations, and posted signs identifying the camera system. Physical alarms such as infrared detection or motion sensors activated the cameras. Monitored cameras from the pipeline control center or security operations center.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Physical Security and Access Controls	**Intrusion Detection and Monitoring**	**Renewable backup power supply**—Used photovoltaic cells/solar panels to charge batteries for backup power to both CCTV and IDS systems at locations where other emergency power is not reasonably available.
Physical Security and Access Controls	**Intrusion Detection and Monitoring**	**Secure Digital Video Recorder (DVR) equipment**—Secured the station's DVR cabinet to prevent unauthorized access. Maintained the DVR equipment separate from the area being monitored.
Physical Security and Access Controls		**Guard force temporary contracts**—Established and maintained a contract-in-place with a commercial guard company to provide security personnel in a crisis or during heightened threat conditions.
Physical Security and Access Controls		**No signage in front of the building**—Removed the company name and/or logo from the exterior of main buildings to provide security through obscurity.
Physical Security and Access Controls		**PA system for deterrence**—Used a speaker system to directly address suspicious persons on or near company facilities.
Physical Security and Access Controls		**Perimeter No Parking Zone**—Partnered with city government to designate No Parking Zones on any streets adjacent to the perimeter of secure facilities.
Physical Security and Access Controls		**Security patrols**—Utilized guard- or employee-roaming security patrols at company facilities. At accessible unmanned or remote facilities, a minimum semiweekly nonroutine foot and vehicular patrols were required.
Physical Security and Access Controls		**Signage in sensitive areas**—Avoided using signs or labels to identify outside locations and features such as air intakes, fuel supply valves, gas or power distribution locations, and evacuation assembly areas. If building identification was needed, used a number system so the building sign is not associated with its purpose or contents.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Risk Analysis		**Competent persons**—Ensured vulnerability assessments are conducted by individuals who are fully competent based on education, training, or experience, including knowledge in security planning and aspects of the operator's systems. • Internal expertise—Conducted security vulnerability assessments on assets using internal subject-matter experts familiar with both security and pipeline operations knowledge. • External expertise—Conducted SVAs with the assistance of certified, external security professionals. • External Resources—Conducted SVAs with the assistance of external resources such as the Federal Bureau of Investigation (FBI), local law enforcement, or other appropriate resource.
Risk Analysis		**Concurrent assessments—**Included the facility and/or asset security criticality assessment in conjunction with other vulnerability and risk assessments.
Risk Analysis		**Crime index and crime-reporting service**—Incorporated—as part of a threat assessment—the use of a crime-reporting and indexing service that gathers major crime index statistics.
Risk Analysis		**Critical-facility SVAs**—Conducted formal SVAs and security audits at critical facilities on a regular basis.
Risk Analysis		**Dedicated threat analyst**—Employed a threat analyst(s) to research open-source information and network within the intelligence community for threat information that may be of concern. These analysts provided the company security managers with weekly intelligence reports and they can be on-call should a situation arise.
Risk Analysis		**GIS incident mapping**—Utilized GIS software to map incident sites on the pipeline system map. Defined any hotspots or problematic areas observed.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Risk Analysis		**GIS mapping**—Utilized GIS mapping to identify colocated infrastructure and security concerns near company assets.
Risk Analysis		**Internal incident-tracking system**—Maintained a database for the collection and storage of threat information. Analyzed the information housed in the database on a recurring and frequent basis.
Risk Analysis		**Levels of asset criticality**—Used three levels or tiers of asset criticality: TSA defined critical facility, business-critical facility, and standard facility. Conducted annual risk assessments with representatives from each appropriate business unit to validate criticality level based on the current threat environment and asset/facility criticality classifications.
Risk Analysis		**Security reconnaissance**—Conducted regular aerial patrols of pipeline systems utilizing a pilot trained in pipeline-security awareness.
Risk Analysis		**Security Working Group**—Established a Security Working Group (SWG) to assess the criticality of pipeline and cyber facilities. The SWG was comprised of staff from operations, safety, and security and included members from management, field operations, pipeline control-center operations, engineering, and cyber/IT.
Risk Analysis		**Security-incident overview graphs**—Analyzed security-incident trends using graphic modeling that provides a visual interpretation of security incident occurrences.
Risk Analysis		**Security-incident reporting database**—Implemented an incident-reporting system and documented events and threats via an incident-tracking database. Provided a security report to company management on a monthly or quarterly basis.

Primary Security Category	Secondary Security Category	Pipeline Industry Smart Practices Observed by TSA
Risk Analysis		**Security-program metrics**—Developed security-program goals that can be tracked by monthly or quarterly metrics. Provided security summary reports to company management on a monthly or quarterly basis.
Risk Analysis		**Threat information**—Utilized national, state, and local threat-information sources and relationships/partners such as members of the Interagency Sustainability Working Group (ISWG) and Joint Terrorism Task Force (JTTF).
Risk Analysis		**Threat monitoring**—Utilized a private company for day-to-day threat monitoring.
Risk Analysis		**Tiered risk classification of facilities**—Created a risk-assessment matrix including a severity-ranking table to consider threats, likelihood, and severity/consequence. The risk model used was Risk = function (Threat x Vulnerability x Consequence) [R=f(TVC)] equation which is also used by the TSA Pipeline Security Division. Information on this method of determining risk may be found in the National Infrastructure Protection Plan (NIPP) at http://www.dhs.gov/files/programs/editorial_0827.shtm.