Transportation
Security
Administration

PIPELINE SECURITY SMART PRACTICES

PIPELINE SECURITY
TRANPORTATION SECTOR NETWORK MANAGEMENT (TSNM)
AUGUST 2006

EXECUTIVE SUMMARY

U.S. hazardous liquids and natural gas pipelines are critical to the nation’s commerce and economy and, as a consequence, they can be attractive targets for terrorists. Before September 11, 2001, safety concerns took precedence over physical and operational security concerns for a majority of pipeline operators. Security matters were mainly limited to prevention of minor theft and vandalism. The terrorist attacks of 9/11 forced a thorough reconsideration of security, especially with respect to critical infrastructure and key resources. Pipeline operators have responded by seeking effective ways to incorporate security practices and programs into overall business operations.

The Transportation Security Administration (TSA) Pipeline Security Office examines the state of security in the pipeline industry, most notably through its Corporate Security Review (CSR) program. A CSR encompasses an on-site review of a pipeline operator’s security planning and the implementation of those plans. Program goals include developing first-hand knowledge of security measures in place at critical pipeline sites, establishing and maintaining working relationships with key pipeline security personnel, and identifying and sharing smart security practices observed at individual facilities.

The “Pipeline Security Smart Practices” reflect the application of data collected from CSRs conducted since the inception of the program in the fall of 2003. A qualitative and quantitative examination of this data, coupled with literature research of pipeline security measures, identified smart practices operators can institute to promote an effective security program. The practices cover a range of topical security areas, including risk and vulnerability assessments, security planning, threat information, employment screening, facility access controls, physical security, intrusion detection, monitoring systems, SCADA and information technology security, awareness training, incident management planning, drills and exercises, and cooperation with regional and local partners, such as law enforcement and other pipeline operators.

This document is intended to assist the hazardous liquid and natural gas pipeline industries in their security planning and the implementation of security measures to protect their facilities, their assets, their people, and the public. TSA will periodically review these practices to maintain their viability in the face of developments in the threat environment and advances in security technology. The overall objective of this effort is to enhance the security posture of the pipelines transportation mode by identifying and sharing practices that reduce risk and enhance security.

TABLE OF CONTENTS

OVERVIEW OF PIPELINE SECURITY IN THE UNITED STATES

Hazardous liquid and natural gas pipelines are critical to the health of the U.S. economy. The nation cannot easily heat homes, operate industrial equipment, fuel various air and surface vehicles, or generate adequate levels of electricity without the valuable commodities transported across the country via pipelines. Interruption of pipeline service, whether from a natural disaster or a malicious act, could negatively impact the public health, cause environmental damage, and inflict economic havoc on an individual operator, region, and the nation at large. The high value of the products transported cross-country by hazardous liquid and natural gas pipelines makes them a critical component of the nation's transportation infrastructure.

The importance of pipelines to the nation's commerce and economy makes them a potential and favored target for terrorist attacks. Globally, terrorist attacks against pipelines have occurred in Iraq, Nigeria, Columbia, and Russia in recent months. In order to prevent or reduce the impact of such attacks in the U.S., improving and enhancing the security of the nation's pipeline system is a heightened priority for both government and private industry.

Safety priorities took precedence over physical and operational security concerns for a majority of pipeline operators prior to the terrorist attacks of September 11, 2001. Security matters were mainly limited to prevention of minor theft and vandalism. Since 9/11, pipeline operators have revisited the issue of security and have made the effort to determine how to better incorporate security practices and programs into overall business operations. The pipeline industry's existing security plans and procedures are based on voluntary guidelines developed and issued by the federal government. The industry largely supports the security guidance and most operators have security plans in place. Operators are taking a balanced approach to security planning due to resource limitations, such as finances and personnel. Many companies are trying to identify multiple benefits to security planning, such as:

- Providing protection against other non-terrorism threats, such as vandalism, criminal activity, and workplace violence;
- Providing operational benefits and mitigation strategies for outages caused by natural disasters or construction related incidents; and
- Maintaining public confidence in the ability of the operator to provide needed goods to serviced communities.

TSA Pipeline Security is currently determining the state of security in the pipeline industry, most notably through its Corporate Security Review (CSR) program. A CSR encompasses an on-site review of a pipeline operator's security planning and the implementation of those plans. The program began in April 2003 and emphasizes the importance of security management practices and policies. Program goals include developing first-hand knowledge of security measures in place at critical pipeline sites, establishing and maintaining working relationships with key pipeline security personnel, and identifying and sharing smart security practices observed at individual facilities. The program's principal objectives are:

- Providing domain awareness of security measures throughout the transportation industry;
- Demonstrating the ability to project a consistent and vigilant approach to the industry-wide implementation of security measures;
- Promoting outreach to the major pipeline stakeholders as a means to ensure constant communication; and
- Emphasizing the necessity for industry to implement strong employee awareness programs for security related issues

The CSR mission is to reduce vulnerabilities to the nation's transportation system by providing stakeholders with security guidance and advice for use during heightened alert levels and in everyday operational practices. To this end, the CSR Program provides a means to encourage constant security-related improvements and enhancements to the pipeline industry.

The *"Pipeline Security Smart Practices"* reflects data collected during over 45 50from CSRs conducted by the Pipeline Security Office since the fall of 2003 to date. A qualitative and quantitative examination of this data, coupled with literature research on security issues for various types of pipelines, identified smart practices operators can institute to promote an effective security program. The following document details those security practices that help enhance and improve the security of the pipeline industry.

RISK ASSESSMENTS, VULNERABILITY ASSESSMENTS, & SECURITY PLANNING

It is prudent to conduct vulnerability and risk assessments before performing any security planning. Vulnerability assessments help operators identify critical assets and exploitable security weaknesses. Risk assessments help operators determine the probability of a particular threat occurring to an asset and the consequence of potential damage to the asset if the threat were to occur. Vulnerability and risk assessment recommendations are often used as a guide for development and implementation of a security plan and help justify expenditures for security improvements and enhancements to senior company management. A security plan supported by senior management fosters a security culture within a company and helps to reinforce the importance of security in day to day operations.

Pipeline vulnerability and risk assessments include:

- Identifying threats to assets, dependent infrastructure, employees, information, and finances;
- Pinpointing specific assets that may be impacted by identified threats and the relative criticality of these assets; and
- Determining the likelihood a threat may occur.

Typically, vulnerability and risk assessment results enable a pipeline operator to consider how many of the recommendations to implement when weighed against the level of protection that is desired. When prioritizing security investments, pipeline operators need to balance the limited resources available to implement enhancements with the public’s demand for enhanced security.

Smart Practices

Smart practices in regard to assessments and security planning include:

- Conducting periodic vulnerability and risk assessments of company assets;
- Identifying whether the company owns any critical assets, as characterized by the criticality definition in the federal pipeline security guidelines;
- Documenting findings and recommendations of vulnerability and risk assessments;
- Restricting and tracking access to company vulnerability and risk assessments;
- Reassessing criticality periodically in conjunction with vulnerability and risk assessments;
- Identifying operational business critical assets and reassessing their importance periodically in conjunction with vulnerability and risk assessments;
- Developing a security plan that incorporates findings from company vulnerability and risk assessments;
- Designating a corporate security officer or corporate security team in the security plan;

- Creating a centralized filing and tracking system of the security plan original, copies, and relevant assessments;
- Gaining senior management support of the corporate security plan and proposed security upgrades;
- Obtaining adequate monetary resources and staffing to implement the plan; and
- Reviewing and updating the security plan annually.

THREAT INFORMATION

Terrorist attacks on pipelines can be accomplished a variety of ways and have disastrous effects on the operations of a pipeline system(s). For instance, simultaneous, direct bombings to several critical pumping or compressor stations could be crippling to an operator, resulting in significant property damage, economic loss, and long-term outages. Similarly, destruction of electrical power grids servicing a facility, while not directly impacting the facility, could reduce or halt product deliveries for an indefinite period of time. In each instance, the public may question the operator's ability to prevent similar attacks and to continue providing needed commodities (i.e. oil and natural gas). Consequently, receipt of pertinent and timely threat information is critical to pipeline operators if they are to protect their assets and facilities from potential terrorist attacks.

Threats to pipelines could include:

- Vehicle Born Improvised Explosive Device (VBIED);
- Improvised Explosive Device (IED) or other explosive devices;
- Standoff Weaponry
- Arson;
- Vandalism;
- Sabotage;
- Chemical Agent Introduction;
- Supervisory Control And Data Acquisition (SCADA) and Information Systems Hacking;
- Loss of Interdependent Infrastructure (electrical, telecommunications); and
- Workplace Violence.

Security threats to a pipeline may come from inside or outside a company. An inside threat usually originates from an individual who has access to a company's facilities, assets, or information systems as part of his or her daily work activities. An insider's presence usually does not raise suspicion and, as a consequence, is hard to detect until it is too late. Insider threats can stem from pipeline system employees, vendors, or contractors.

An outsider threat is derived from a person not normally allowed access rights to pipeline facilities, assets, or other associated infrastructure. Questions may be raised if such a person is seen on property belonging to the operator. A pipeline company should consider mitigation strategies that address both insider and outsider threats when developing its corporate security plan.

The Homeland Security Advisory System (HSAS) can be used as a guide for gauging where to set the appropriate company threat level in response to the types of threats referenced above. Federal guidelines released to the industry in 2002 advised operators to create threat level response plans that detail specific security measures to undertake upon a change to the HSAS. It is suggested that pipeline operators develop threat level response plans that correspond and complement the HSAS.

Smart Practices

Pipeline smart practices for threat level responses include:

- Adopting a company threat level response system similar to the HSAS;
- Documenting processes the operator will conduct when evaluating threat information and establishing the company operational threat level;
- Coordinating company threat level changes with regional response authorities;
- Collaborating with other area pipeline operators to establish consistent threat level responses;
- Maintaining documentation of all threat level changes and responses;
- Securing government security clearances for company personnel in charge of security in order to facilitate threat information receipt; and
- Formalizing processes for transmitting pertinent threat information to employees.

EMPLOYMENT SCREENING

One of the most difficult security threats to deter is an employee with malevolent intents. Due to employee proximity to sensitive information and assets, it is important to identify potential threats as early as possible. Thorough background screening can assist in detecting candidates who could pose a security risk.

Smart Practices

To help prevent this type of threat, several identified employment screening smart practices include:

- Conducting criminal, employment, education, and reference checks on all new employees;
- Implementing additional background checks, as appropriate, for certain organizational positions and on employees with access to secure areas;
- Applicable checks should be retroactive to 7 years, at a minimum;
- Screening the criminal history of existing employees on a periodic basis;
- Developing and implementing personnel policies that enable the company to terminate an offer of employment, or an existing employee, if an individual is found to have committed a crime; and
- Requiring all written contracts stipulate that personnel provided to the company undergo specific pre-employment checks.

Some of the better credentialing programs observed included screenings that encompassed most or all the above listed practices. One operator told TSA that it conducts background investigations retroactively to 1975. Another operator told TSA that it ties its employee background re-screening program to its random drug testing program. Operator background screenings are conducted either in-house, via the company human resources department, or through a third-party agency that specializes in pre-employment checks. Regardless of the means an operator chooses to conduct background investigations, it is crucial that an operator ensure the screenings are adequate and thorough.

BADGING & ACCESS CONTROLS

It is vitally important that pipeline operators control access to facilities to prevent the unauthorized admittance of individuals with the potential to cause harm. To achieve this objective, pipeline operators should implement procedures to monitor all persons entering and exiting company facilities. Employee badging, access controls, and access policies allow for the movement of authorized personnel and materials into and out of facilities while simultaneously deterring movement of unauthorized personnel or contraband.

Card reader access control systems are the most common method of controlling access to pipeline facilities and assets. Additionally, many operators are also reliant on key locks and a key control system that can track key issuance, loss, and collection. Company issued photo identification credentials with access control system privileges are frequently used by pipeline operators to verify an employee's identity and to control access to facilities. Many access control systems can be monitored on common PC workstations and newer card reader systems even have the ability to integrate with payroll, information technology, and human resources databases.

Smart Practices

The following are identified badging and access control smart practices that pipeline operators can undertake:

- Issuing employee and contractor badges only after background checks have been completed with favorable results;
- Displaying an employee's name and current photo on issued access control cards;
- Encoding all issued badges with the appropriate level of access necessary for an employee or contractor to perform job duties;
- Distributing distinctively colored badges encoded with restricted access controls to visitors;
- Requiring employees, contractors, and visitors to wear badges at all times;
- Limiting employee access (through key control or programmable access control system) to only areas needed to fulfill job requirements;
- If access controls utilize a programmable personal identification number (PIN), require the PIN to contain 8 or more alpha-numeric characters;
- Using anti-passback software to prevent employees from giving their cards or PIN numbers to someone else to use;
- Implementing a company-wide badge access control monitoring program;
- Developing and executing a badge collection and deactivation policy for employee and contractor termination, resignation, or dismissal;
- Escorting all visitors, including employee guests, vendors, the general public, and contractors, especially when visiting critical facilities;
- Providing a secure lobby/waiting area for visitors;
- Limiting the number of employees with keys;

- Using patent keys to prevent unauthorized duplication; and
- Implementing a key issuance tracking and return system.

A pipeline operator’s badging program can be integrated into other company programs outside of its security program. One reviewed pipeline operator tied its badging program to its health and wellness program by detailing employee medical alert information on individually issued badges. The same company also tied its badging program to its safety program by requiring all new hires watch a safety and quality assurance video before receipt of company credentials. Such practices are certainly useful and desirable and do not interfere with access control objectives. However, the most important element of a badging and access control program is the strict adherence to policies and procedures for updating, issuing, replacing, and deactivating badges. A badging and access control program will not be effective if these policies are not practiced and followed.

VEHICLE CHECKPOINTS

The purpose of vehicular checkpoints is to screen vehicles prior to accessing a facility. Pipeline operators should consider implementing some form of vehicle inspection at company identified critical or business-critical facilities and assets.

A simple vehicular checkpoint system can consist of a gate with an intercom and a remote closed circuit television (CCTV) camera. When a vehicle approaches the gate, the driver must request permission to enter the facility using the intercom. Security staff or other pipeline personnel must then visually confirm the identity of the visitor through a workstation monitor displaying the CCTV camera image. If an operator requires that employees be allowed quick access to vehicle controlled facilities, an exterior access card reader can be installed just outside a secured gate. A more comprehensive vehicular checkpoint system could include a guardhouse located at the entrance to a controlled facility. A security officer would screen all vehicles prior to allowing them to enter the site. Any vehicles or persons with no identified purpose for visiting the facility would be denied access and the attempted breech would be reported to local law enforcement through the proper company incident reporting channels.

Smart Practices

For companies employing some method of vehicular inspection, TSA has identified the following smart practices:

- Installing crash resistant gates at the entrance to restrict vehicular access to controlled facilities;
- Placing vehicle barriers around facilities (i.e. jersey barriers, ditches, etc.) or installing fencing cables;
- Utilizing entrance barriers at critical facilities that resist vehicular ramming, such pop-up bollards, hydraulic ramps, wedges, or plate barriers
- Mounting sufficient lighting to enhance visual observation at vehicular entrances;
- Minimizing gate access at vehicular controlled facilities;
- Setting a location to detain unauthorized persons and vehicles at controlled facilities, if possible;
- Placing a telephone or intercom in all vehicular guardhouses, if used;
- Equipping vehicular entrance guardhouses within a bullet resistant and weather protected enclosure; and
- Exempting authorized personnel with appropriate credentials (both personal and vehicular) from screening requirements.

Deliveries are a particularly difficult challenge for pipeline facilities. Pipeline operators should require that suppliers coordinate delivery drop offs in advance and that a delivery manifest and driver name be provided. To implement this security approach, an operator could adopt a procedure that requires faxed or electronically transmitted copies of delivery bills and driver identification be sent to a company representative prior to any delivery. Delivery trucks should be met by trained security staff or other company personnel and any unverifiable, unscheduled, or late deliveries should be refused. Operators should consider keeping detailed logs of deliveries and pick ups, including driver information and destination. Similar procedures can be performed prior to allowing a vehicle to depart a facility. Pipeline operators may also want to consider inspecting delivery trucks and vehicles for theft or contraband prior to leaving a site.

PHYSICAL SECURITY

Simple protective measures such as lighting and perimeter fencing may deter petty criminals looking for an opportunity to commit a crime. Deterring terrorists often requires additional, more costly, security investments than measures used to deter common crime. Enhanced physical security measures are often utilized only at facilities and assets that, if impaired, would significantly affect business operations. All reviewed pipeline operators use physical security barriers to varying extents to protect company facilities and assets, often using a combination of measures. When selecting security barriers and devices to secure company assets, tamper-resistant materials and components should be considered, including composite plastics that resist graffiti and cages or other protective fittings.

Operators are finding that once physical security measures are implemented, they are also protected against other non-terrorism operational threats, such as vandals and disgruntled employees. Companies are also discovering other operational benefits associated to heightened security also prove useful during a natural disaster or construction related incidents and help to restore system operations and service more quickly. Security measures that provide multiple operational benefits such as noted above helps to maintain public confidence in the reliability of the pipeline system and its continued service to a community or region.

Smart Practices

Pipeline smart practices for physical security include the following:

- Providing adequate nighttime lighting at all company facilities, especially at designated critical, unmanned, or remote facilities;
- Mounting perimeter lighting, if used, at least 20 feet off the ground from at least one or more pole locations, in order to prevent the lighting from being tampered with or vandalized;
- Designing company entrances to be well lit, well defined, and highly visible to the public and pipeline employees;
- Creating “clear zones” that extend 6 feet or more from facility perimeters that are free of tall shrubs and trees;
- If visual screening of a facility is required by local authorities, use landscape plants that prevent easy passage (i.e., thorned shrubs) and that do not obstruct lighting;
- Installing high quality security fencing around facility perimeters, such as chain link fencing with a 3-strand barbed or razor wire outrigger;
- Avoiding use of fencing, landscaping, or walls that might provide block vision into a facility and provide hiding places along the perimeter;
- Establishing a 25-foot or more stand-off distance from perimeter fencing to main facility, if possible;
- Providing door access at both the front and back of buildings to facilitate patrols;
- Regularly maintaining the exterior of all facility and assets and conducting repairs as necessary, to include lighting, fencing, gates, doors, locks, and windows;

- Locating dumpsters and trash barrels as far from assets as practical;
- Restricting access to roofs;
- Ensuring facilities can not be accessed by loading docks, poles, ladders, and skylights;
- Closing facility entrance gates with tamper proof, weather resistant, shackle-protected padlocks to prevent possible attempts at picking, cutting, sawing, prying, hammering, and cutting;
- Locating pipes, valves, meters, and other appurtenances that may be damaged or tampered with behind sturdy fencing or panels;
- Ascertaining signage at all facilities is hanging beyond easy reach and includes an appropriate telephone number to report any unusual or suspicious activity;
- Burying or otherwise protecting conduits and wires carrying electrical supply, telecommunications, and alarm signals; and
- Scheduling major annual maintenance activities during low demand periods to reduce the impact of system vulnerabilities.

The most common physical security measures TSA has observed pipeline operators use include chain-link fencing and jersey barriers. As mentioned above, although all reviewed pipeline operators have installed physical security barriers, lack of regular maintenance diminishes their effectiveness, particularly fencing. During the CSR program, TSA has found the most important component of an effective physical security program is the emphasis on the proper implementation of that plan and the upkeep of the barriers used.

INTRUSION DETECTION ALARMS & CCTV MONITORING

It is important to assess alarms quickly and accurately, without compromising the safety or security of pipeline personnel or assets. Intrusion detection alarms and closed-circuit television (CCTV) systems can be effective tools for detecting, classifying, and identifying potential and actual security breaches and are an important component of an operator’s security program.

The following should be considered when deciding to invest in a CCTV system:

- Simplicity of use;
- Means to integrate new technologies into the system as needed or able;
- System compatibility;
- Availability of a service plan for system maintenance and quality control issues;
- CCTV monitoring capability (i.e., personnel, monitors, and workspace resources needed);
- Backup power sources needed and ability to secure and effectively install and store resources;
- Ability to adequately mount cameras so that they operate effectively; and
- Ample day and nighttime lighting in the area(s) of installation.

Several technologies allow for camera viewing in low light situations, including black/white switching cameras, infrared illuminators, and thermal imaging cameras. It is important that the deployment of low light CCTV technology account for the specific needs of cameras used. A one-size-fits-all approach will not work. Different cameras in a CCTV system may have different lighting needs that must be identified prior to installing any one particular type of low light technology. Other important considerations in regards to CCTV systems concern whether the cameras are fixed position or have pan, tilt, and zoom (PTZ) capabilities. Fixed position cameras are mounted in a permanent position and, though they cannot move or pan to capture images, are good for detection surveillance. PTZ cameras are mounted to allow for rotating, panning, tilting, and zooming capabilities, and are often used for site surveillance and alarm assessment needs. However, there are cost differences with the two types of cameras. Cameras with PTZ capability may be as much as four times more expensive than fixed cameras due to the motor needed to operate the camera. Additional maintenance requirements may pertain as well.

Regarding intrusion detection alarms, there are several different types of alarm sensors in use today, including boundary penetration, buried line, and fence mounted sensors. Boundary sensors detect an intrusion across an interior boundary such as a door, window, or hatch. The most common boundary sensors are door switches, glass break sensors, and beam sensors. Buried line sensors rely on sensing an intruder via means of a buried cable underneath the ground. Fence mounted sensors are mounted to a fence in order to detect climbing or cutting. Pipeline operators should consider the capabilities and limitations of each type of sensor prior to installing one or more at a facility. All alarms that are installed should be remotely monitored at either a system control or security operations center.

Smart Practices

Pipeline smart practices in regard to the use of intrusion detection alarms and CCTV monitoring include:

- Using audible and visual intrusion detection alarms at all company designated critical facilities and, if possible, all unmanned and remote facilities;
- Installing alarms on doors and windows that provide access to critical areas so that any unauthorized entry will alert appropriate alarm monitoring personnel;
- Using CCTV with motion detection capabilities at all company designated critical facilities and, if possible, all unmanned and remote facilities;
- Integrating alarm capabilities into installed CCTV monitoring systems;
- If no third party security monitoring service is utilized, ensure intrusion detection alarms and CCTV systems at a computer workstations in an operator's security or SCADA control center;
- Positioning security cameras at vehicle gate entrances in order to view vehicles, drivers, and license plate numbers;
- Locating security cameras outside building entrances to monitor persons entering and exiting facilities;
- Programming PTZ cameras with a minimum of three preset viewing conditions;
- Providing, at a minimum, a 4-hour battery back-up or alternate power source, to all security alarm and monitoring systems;
- Storing security system alarms and CCTV system images (either digital or taped) for at least 30 days;
- Mounting security alarm and monitoring systems to a high quality, sturdy object in order to maximize effectiveness;
- Conducting annual reliability tests of intrusion detection and CCTV monitoring systems; and
- Contracting a reputable firm to provide repair service for CCTV system.

Some operators with CCTV systems use digital video recording devices to store video images. Benefits to a digital record system include elimination of media tapes, reducing physical storage space, and the ease of search-and-playback functions. A variety of different security systems and components are commercially available. Before implementing a security system, it is important to understand the characteristics and requirements of the area and facility to be protected. With this understanding, details and specific criteria can be developed to specify exactly how the security system should be implemented.

GUARD SERVICES

Guards provide pipeline operators with extra facility protection. Use of guards enables pipeline employees to focus on daily operations while guard personnel focus exclusively on security concerns. Many pipeline operators use contract guard services or off-duty local law enforcement for patrols and guard station duty either regularly or during periods of heightened alert. Guards are usually employed to check for employee badges, inspect vehicles, patrol facility perimeters, and to look for any unusual or suspicious activity.

Smart Practices

Identified smart practices regarding guard services include:

- Hiring guards trained in a variety of screening techniques and system security operations, and knowledgeable in the tactics terrorist use to attempt to avoid detection;
- Tasking guards to conduct frequent, random, physical and vehicular perimeter patrols at manned facilities;
- Requiring guards conduct varied physical and vehicular patrols of accessible unmanned or remote facilities, bi-weekly, at a minimum;
- Training guards on company emergency preparedness plans and company response resources;
- Requiring guards to participate in company exercises, drills, and tabletop exercises; and
- Establishing communications, record keeping, and standard operating procedures for guard personnel to follow.

SCADA & INFORMATION TECHNOLOGY SECURITY

Supervisory Control and Data Acquisition (SCADA) networks are used to control and operate the pumps, valves, and instruments that control the movement of goods in a pipeline system. These networks were initially designed to maximize functionality and operating ease with minimal security precautions, and consequently, are an attractive target for remote cyber attacks.

Like SCADA networks, information technology (IT) systems are increasingly more vulnerable to cyber attacks. Pipeline employees need 24-hour a day access to company information systems in order to operate the gas system and promote efficiency. This needed access increases the opportunities for intruders to hack into and possibly affect the integrity of a company's IT system.

Smart Practices

To offset this potential threat, identified smart practices for SCADA and IT security include the following:

- Formalizing data protection guidelines, protocols, and policies;
- Isolating the SCADA control and vital company information technology networks from other network connections;
- Installing virus and firewall detection protections on all network systems;
- Configuring all operating systems and servers for daily virus and security patch updates;
- Auditing firewall logs for unauthorized entry attempts;
- Conducting firewall system evaluation and penetration testing on a recurring basis to ensure optimal system performance;
- Training pipeline employees with access to SCADA and information technology systems on all data protection guidelines, protocols, and policies;
- Requiring employees use unique user IDs and passwords to access SCADA and computer systems;
- Programming logon privileges to match responsibility level;
- Using logon credentials, track and regularly audit actions and changes made to operating systems;
- Ensuring all network system passwords are not set to default settings;
- Immediately removing user accounts upon voluntary or involuntary terminations;
- Limiting wireless networking and ensuring authorized wireless networking is protected by the highest encryption levels possible;
- Configuring network systems to logout after a certain amount of time of inactivity;
- Programming the SCADA control network to a set point range to protect the system from harmful, out of range alterations;
- Securing access to the SCADA control center with access control devices or keys;
- Locking SCADA servers in a controlled and monitored area;
- Periodic SCADA system vulnerability assessment;

- Ensuring there is a back-up power source for all servers, network components, and vital workstations;
- Establishing and testing the back-up SCADA relocation site; and
- Conducting regular system back-ups, copies of which should be kept at the SCADA relocation site.

In addition to the above mentioned practices, TSA has observed SCADA network security protections that also encompass field remote terminal units (RTU). Field RTUs exchange, monitor, and control information in "plain text." Pipeline operators are dependent on RTUs to interact with remote SCADA components. If unencrypted RTU broadcasts are intercepted, they can easily be retransmitted with different and potentially harmful information. To mitigate this risk, TSA has identified the following smart practices in regard to RTU security:

- Hardening remote SCADA control system units with lockable enclosures;
- Installing signal alarms to detect tamper attempts;
- Encrypting radio traffic between RTUs and the master control unit; and
- Ensuring there is a back-up communications server installed.

Y2K concerns in the late 1990's stressed the importance of SCADA and IT security to pipeline operators. Pipeline operators invested time and money into better securing computer networks in preparation for possible Y2K data issues. The terrorist attacks of September 11th, 2001 have caused pipeline operators to reexamine the security of computer networks.

The key to deterring cyber attacks is strong and enforced network data protection policies and procedures that reduce the risk for potential damage by limiting physical and electronic anonymous access privileges. Given that SCADA and IT computer networks have inherent vulnerabilities that can be exploited, it is prudent that operators implement all applicable practices mentioned above to maintain and protect the integrity of company network systems. Where a distinct entity is involved in network security, such as a local municipality for publicly-owned distribution utilities, close coordination with that entity's IT department or representative on network security issues is critical.

SECURITY AWARENESS TRAINING

One of the most cost-effective security practices a pipeline operator can pursue is security awareness training for employees and contractors. New employee orientation sessions, if offered, are an easy way to initiate security awareness training and to introduce some of the company's security policies.

Smart Practices

Smart practices for employee security awareness training should include discussion on the following subjects:

- Operational security (i.e., threats, surveillance techniques, terrorist counter surveillance techniques, etc.);
- Threat level response measures and policies;
- Company physical security measures (i.e., access controls, badging, etc.);
- Conflict management and communication training (handling phoned-in bomb threats, etc);
- Personal protection training (shelter in place protective measures, etc); and
- Information technology and data protection policies.

Employee security awareness training should be a dynamic program rather than a one-time offering. Continued security awareness training can be offered in a variety of formats, from company newsletter articles to email updates, computer-based training applications, and staff meetings. Additionally, pipeline operators should implement a security training quality assurance program to ensure that new and evolving threats are integrated into training for employees.

For many operators, an integrated computer based security training program may be the most desirable format in which to provide security awareness to employees, due to its relative ease of implementation and tracking and retraining abilities. However, other training formats should also be considered and utilized to reinforce a culture of awareness.

SECURITY INCIDENT MANAGEMENT PLANNING

Security incident management planning specifies how pipeline operators will respond to, recover from, and conclude security-based emergencies, including the way business will proceed during and after an incident and how any damage will be assessed and repaired. Clear and timely security response activities can save lives, property, and credibility. A good security plan documents the notification procedures to be followed in the event of a suspected threat and address specifically how to report the incident, who to notify, and what, if any, response should be undertaken. All employees who might be involved in the response to an incident should be trained as to proper response protocols and procedures.

Smart Practices

Smart pipeline practices for incident management planning include:

- Providing all pipeline employees and contractors with security incident response procedures, to include bomb threats, pipeline system or asset destruction, unauthorized entry, workplace violence, SCADA or IT attacks, health and safety emergency, or an environmental contamination threat;
- Clearly defining notification policies and assuring they are understood by all employees and contractors;
- Identifying appropriate local, state, and federal agencies to contact upon a suspected terrorist incident and provided updates when warranted;
- Creating 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 (incident management team, utility personnel, mutual aid partners, media contacts, and affected landowners surrounding a site, among others);
- Logging and tracking copies of the incident management plan so that copies can be updated as needed;
- Establishing an off-site alternate operations center for security incident response coordination;
- Stocking the alternate operations site with adequate supplies, including telephones, computers, faxes, radios, system maps, standard operating procedures (SOPs), table, chairs, and basic office supplies, in addition to other basic provisions;
- Establishing a back-up communication system for use in the event of a power loss or other system failure; and
- Creating an incident report log and records preservation system to serve as an official record of actions and lessons learned for the post-incident review.

The better established the incident response and communications protocols are before an emergency, the more efficient and successful the response will be in a security crisis. Many of the listed practices are currently being used by pipeline operators, and have been for some time. Many operators integrate security incident reporting procedures into their safety programs, or have a documented section in their company security plan addressing the topic. However, it would be prudent for all pipeline operators to document incident management planning and procedures in the company security plan.

DRILLS, EXERCISES, AND REGIONAL COOPERATION

Reaching out and establishing a cooperative relationship with regional Federal, state, and local law enforcement agencies, as well as local right-of-way landowners and other area pipeline operators, is a very effective way of enhancing the security of facilities and assets, especially those at unmanned locations. Mutual aid and regional cooperative relationships help establish planning, response, and recovery practices that are complementary and beneficial to all regional stakeholders.

Smart Practices

Smart pipeline practices in the area of drills, exercise, and regional cooperation include:

- Establishing liaison, mutual aid, and resource sharing relationships with local law enforcement, first responder agencies, and other area pipeline companies;
- Engaging local police, first responders, interested pipeline operators, and landowners in company sponsored exercises and drills;
- Expressing interest in participating in drills and exercises sponsored by other local stakeholders; and
- Communicating security information to interested right-of-way landowners through a Neighborhood Watch Program.

Drills and exercises are critical if an operator’s incident response plan is going to be successful during response to an actual security incident. Drills and exercises also provide a forum for pipeline personnel and local area first responders to interact with one another and gain familiarity with each other’s capabilities, procedures, and needs during a response to an incident. TSA has observed many noteworthy approaches operators have employed to engage regional and local law enforcement agencies in mutual aid and cooperation. Such examples include pipeline operators that invite local on-duty police officers into company facilities for a cup of coffee or offer company space to park off-duty police cruisers.

Local right-of-way landowner outreach has also been impressive. Most pipeline operators realize the importance of engaging landowners in a cooperative relationship and conduct landowner outreach via written communications, text messaging, email, and the local media. One of the more striking methods identified for landowner outreach involved an operator sponsored website for right-of-way landowners, with incentives to the landowners for accessing and using the site.

Mutual aid relationships among pipeline operators are understandings rather than formal agreements. Given the interdependency of much of the Nation’s hazardous liquids and natural gas pipeline systems, owner/operators recognize it is possible that any attack on a pipeline would have cascading effects throughout the system. It would be sensible to document these understandings to ensure that aid and assistance will be received in a prompt and timely manner that does not unduly strain one operator over another.

CONCLUSION

This document is intended to assist hazardous liquid and natural gas pipeline operators in security planning and the implementation of security measures to protect their facilities, their assets, their people, and the public. The TSA does not expect the content of this document to replace security measures already implemented by individual companies or to offer commentary regarding the effectiveness of individual operator efforts. The agency also does not guarantee that any of the measures will completely eliminate possible acts of vandalism, violence, or terrorism.

There is no "one size fits all" way to deal with security planning and it is often independent of the size or throughput of a pipeline system. Security planning and implementation needs to be consistent with a number of factors, including:

- Funding;
- Community restrictions;
- System design and redundancy;
- Operational constraints; and
- Staffing resources.

Each pipeline operator should find a customized solution that fits its level of threat, organizational culture, and financial situation. Operators should consider the following when planning for security:

- Integration of operations and design strategies into the security planning;
- Straightforward solutions; and
- Solutions that provide multiple benefits

A cost-effective approach to developing and implementing a security program is to use in-house resources and assets in all stages of the company's security planning. Understanding the in-house factors that could potentially affect security planning is vitally important to the development of an effective and efficient security program. Additionally, pipeline operators are limited by the funding available for security upgrades. Identification of security measures that provide multiple benefits across two or more areas of operational concern is a useful approach to dealing with security funding issues. A pipeline operator need not create a financial burden, hinder existing operations, or require an overhaul of the pipeline system to achieve a balanced security plan. A simple and practical approach to security planning is the desired outcome for a pipeline system.

Based on continuing experience in the CSR Program and engagement with the pipeline industry, TSA will periodically review these practices to maintain their viability in the face of developments in operating conditions or the threat environment. The constant objective is to enhance security posture throughout the pipelines mode by identifying and sharing practices that reduce risk and enhance security.

REFERENCE MATERIAL

1. Chicago Metropolitan Area Critical Infrastructure Protection Program, *Planning for Natural Gas Disruptions, Critical Infrastructure Assurance Guidelines for Municipal Governments*, Dec. 2002.

2. U. S. Department of Energy, "Lessons Learned from Industry Vulnerability Assessments and September 11th" [http://www.naseo.org/committees/energysecurity/energyassurance/stern.pdf].

3. Interstate Natural Gas Association of America Web Site, [www.ingaa.org].

4. Department of Transportation, "*Pipeline Security Information Circular*", September 5, 2002.
5. Department of Transportation, "*Pipeline Security Conditions and Measures*", September 2002.

6. National Association of State Energy Officials, "State Energy Assurance Guidelines" [http://naseo.org/committees/energysecurity/documents/EAGuidelines.pdf]

7. *Survey Assesses Vital Services*, ASIS Security Management, Nov. 2005.

8. *Securing Oil and Natural Gas Infrastructures in the New Economy* [http://securitymanagement.com/library/NPC_Tech0901.pdf].

9. American Public Gas Association Web Site, [www.apga.org].

10. The New Jersey Petroleum Council and the American Petroleum Institute, *Oil and Natural Gas Industry Security Assessment and Guidance*, January 2002. [http://www.state.nj.us/dep/rpp/download/NJ%20Best%20Practices%20Petroleum%20Sector%20-%20Public.doc].

11. Missouri Security Panel, *Utility Committee Final Report*, January 30, 2002. [http://www.psc.mo.gov/publications/homelandfinalnonames.pdf].

12. American Water Works Association, *Security Guidance for Water Utilities* [http://www.awwa.org/science/wise/report/AWWA_Securities/page2.htm]

13. The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003. [http://www.whitehouse.gov/pcipb/physical.html].

14. American Gas Association Web Site, [www.aga.org].

15. *Terrorism Awareness and Protection*, Pennsylvania Commission on Crime and Delinquency, Nov. 2002.
[http://www.pa-aware.org/].

16. *Bio-Terrorism Level Awareness Training*, Kentucky Terrorism Response and Preparedness, University of Kentucky, Nov. 2005.
[http://www.kiprc.uky.edu/trap/bioterrorism.html]

17. Homeland Security Presidential Directive (HSPD)7
[http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html]

18. Homeland Security Presidential Directive (HSPD)8
[http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html]

19. The National Strategy for Homeland Security
[http://www.whitehouse.gov/homeland/book/index.html]

20. American Petroleum Institute Web Site, [www.api.org].

21. *Cross Sector Interdependencies and Risk Assessment Guidance*, National Infrastructure Advisory Council, January 2004.
[http://www.dhs.gov/interweb/assetlibrary/irawgreport.pdf].

22. *Securing Oil and Natural Gas Infrastructures in the New Economy*, National Petroleum Council, June 2001.