Pipeline Security Guidelines

December 2010

Transportation Security Administration

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

1 INTRODUCTION

Under the provisions of the Aviation and Transportation Security Act (Public Law 107-71), the Transportation Security Administration (TSA) was established on November 19, 2001 with responsibility for civil aviation security and "security responsibilities over other modes of transportation that are exercised by the Department of Transportation." To fulfill this mandate in the pipeline mode, on September 8, 2002, TSA formed the Pipeline Security Division within what is now the Office of Transportation Sector Network Management (TSNM).

1.1 Purpose

In executing its responsibility for national pipeline security, TSNM Pipeline has utilized the Pipeline Security Information Circular, issued on September 5, 2002, by the Department of Transportation's (DOT) Office of Pipeline Safety as the primary Federal guideline for industry security. Complementing this document, and also adopted by TSA, was the DOT-issued Pipeline Security Contingency Planning Guidance of June 2002.

Recognizing that the Security Circular required updating, TSA initiated a process to amend the Federal security guidance. After TSA commenced the document revision effort, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, P. L. 110-53 (9/11 Act). Sections 1557 and 1558 of the 9/11 Act directed TSA to review adherence to the 2002 guidance and to undertake other initiatives.

The revised Pipeline Security Guidelines were developed with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties. This document supersedes the Pipeline Security Information Circular and the Contingency Planning Guidance.

The 2002 Circular incorporated by reference the consensus guidance contained in petroleum and natural gas industry association security publications. Building upon these documents, TSA's intention is not to make significant substantive changes to this guidance but to provide explicit agency recommendations for pipeline industry security practices. Based on its Corporate Security Reviews and other information, TSA believes that pipeline operators already employ most of these recommendations in their security plans and programs.

NOTE: Nothing in this document shall supersede Federal regulatory requirements. This document is guidance. It does not impose mandatory requirements on any person. The term "should" means that TSA recommends the actions described.

1.2 Scope

These guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. Additionally, they apply to pipeline systems that transport materials categorized as toxic inhalation hazards (TIH). TIH

materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans as to pose a health hazard in the event of a release during transportation. (See the Hazardous Materials Regulations: 49 CFR parts 171-180.)

Operators of pipeline systems not included in the descriptions above are encouraged to implement the security measures contained herein to the extent appropriate to their particular system.

2 CORPORATE SECURITY PROGRAM

A risk-based corporate security program should be established and implemented by each pipeline operator to address and document the organization's policies and procedures for managing security related threats, incidents, and responses. In addition, each operator should:

- Ensure sufficient resources, to include trained staff and equipment, are provided to effectively execute the corporate security program;
- Assign a qualified primary and alternate staff member to manage the corporate security program;
- Provide TSA with the 24/7 contact information of the primary and alternate security manager, and the telephone number of the company's security operations or control center;
- Develop a corporate security plan as described in Section 3;
- Develop and maintain a cyber/Supervisory Control And Data Acquisition (SCADA) security plan, or incorporate cyber/SCADA security measures in the corporate security plan;
- Develop and maintain security elements within the corporate incident response and recovery plan;
- Monitor Homeland Security Advisory System (HSAS) threat levels and implement corresponding HSAS threat level protective measures; and
- Notify TSA of all security incidents by phone or e-mail as soon as possible. (Notification criteria and contact information are provided in Appendix B.)

Figure 1 identifies the major steps that each pipeline operator should take in creating and implementing a corporate security program and the relevant sections in the guidelines where specific details are provided.

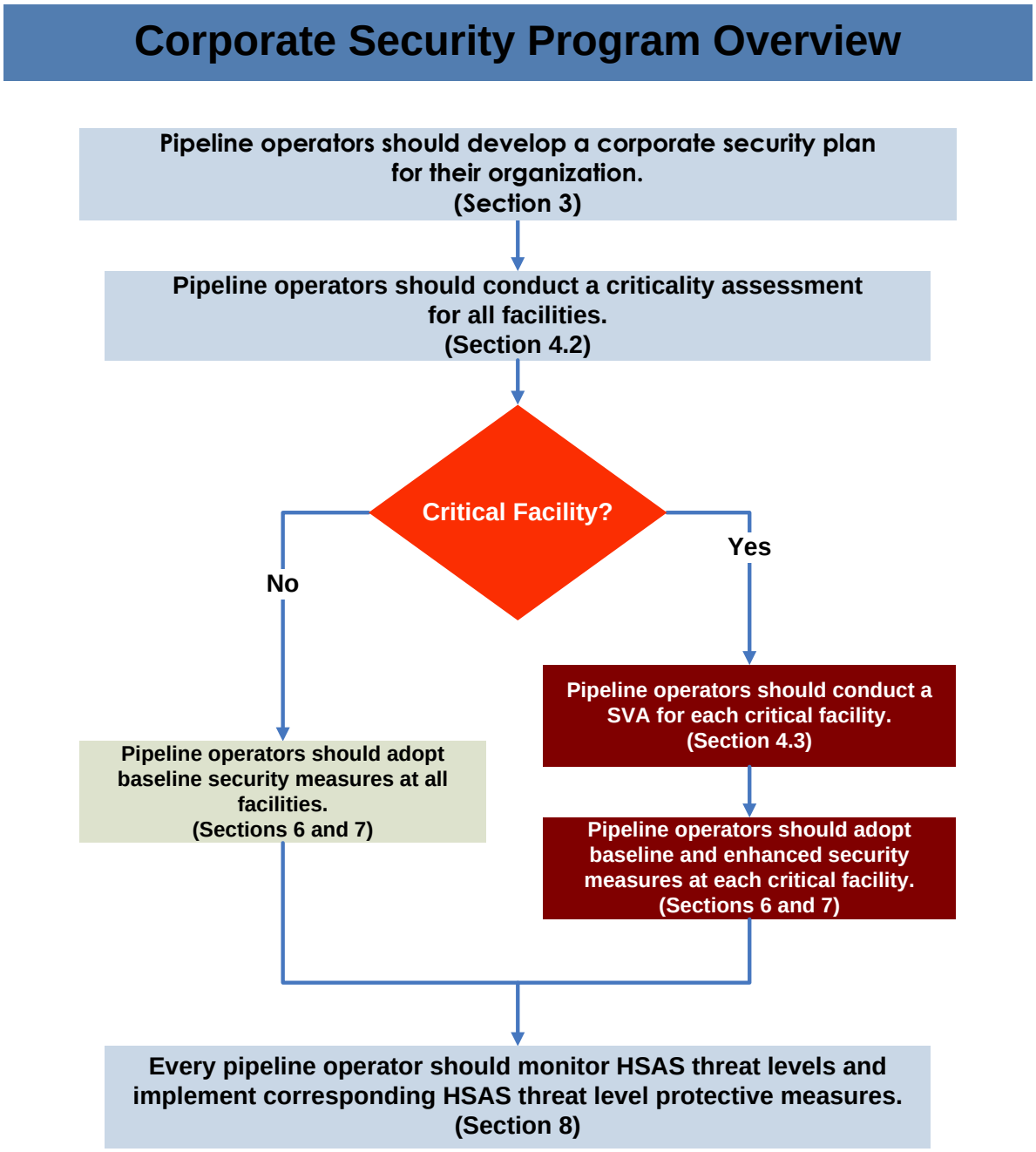

Figure 1: Corporate Security Program Overview

3 CORPORATE SECURITY PLAN

3.1 Introduction

Operators should develop and implement a security plan customized to the needs of the company. The corporate security plan should be comprehensive in scope; systematic in its development, and risk based reflecting the security environment. At a minimum, the plan should:

- Identify the primary and alternate security manager or officer responsible for executing and maintaining the plan;
- Document the company's security-related polices and procedures, to include, but not limited to, methodologies used and timelines established for conducting criticality assessments and security vulnerability assessments (SVAs), if applicable;
- Reference other company plans such as the business continuity plans, incident response and recovery plans;
- Be reviewed on an annual basis, and updated as required based on findings from assessments, significant modifications to the system or any of its facilities, substantial changes to the environment in which it operates, or other significant changes;
- Be protected from unauthorized access based on company policy, and;
- Be available for review and copying by TSA upon request.

3.2 Security Plan Elements

This section identifies and provides a brief description of the recommended elements of a corporate security plan. In developing their plan, operators should incorporate these elements in a format that is most suitable to their organization.

- System(s) Description - Identify the pipeline system(s) to which the plan applies.
- Security Administration and Management Structure - Identify the person(s) primarily responsible for the corporate security program, and describe the responsibilities and duties of personnel assigned to security functions.
- Risk Analysis and Assessments - Describe the methodology used to conduct security risk analysis to include criticality assessments and SVAs.
- Physical Security and Access Control Measures - Describe the corporate policies and procedures employed to reduce security risks throughout the company.
- Equipment Maintenance and Testing - Discuss policies and procedures for ensuring security systems and equipment are maintained and function properly. Information contained in this section may address performance of equipment preventive maintenance as well as inspection and testing of security systems.

- Personnel Screening - Describe policies and procedures for conducting employee background checks, including criteria for disqualification and process for appeal, in compliance with Federal and state laws. Describe company policies for contractor personnel background checks.
- Communications - Describe the policies and procedures employed to ensure effective communication is maintained on both a routine and emergency basis. The description should include, but not be limited to, types of equipment used, communication methods between employees, facilities, and offsite responders, and procedures for notification of government and law enforcement agencies.
- Personnel Training - Describe security training, to include training in security equipment operation, and security awareness training requirements for company personnel, including routine contractors and part-time employees.
- Drills and Exercises - Describe company policies and procedures for conducting security drills and exercises. Establish requirements for after-action reports, communication of lessons learned, and implementation of security improvement efforts based on exercise results.
- Security Incident Procedures - Describe procedures for responding to security incidents and emergencies. Define the types of events that constitute a breach of security, describe the procedures for investigating security incidents, and who should be notified. In addition, the emergency response plan may be referenced in this section.
- HSAS Response Procedures - Describe the operator's escalating protective measures for periods of elevated threat corresponding to the Department of Homeland Security (DHS) HSAS levels.
- Plan Reviews - Describe policies and procedures for the review, validation, and updating of the corporate security plan.
- Recordkeeping - Describe security-related recordkeeping requirements, such as for criticality assessments and SVAs, as well as measures to prevent unauthorized disclosure.
- Cyber/SCADA System Security Measures - Describe the corporate policies and procedures employed to reduce security risks to cyber/SCADA systems and assets throughout the company. If a separate cyber/SCADA security plan is maintained, it should be incorporated by reference.
- Essential Security Contact Listings - List internal and external emergency contact information for reporting and responding to a security incident or suspicious activity.
- Security Testing and Audits - Describe policies and procedures for self-inspection, auditing, and testing of the effectiveness of the company's security plan and procedures, to include documentation of results.

4 RISK ANALYSIS

4.1 Introduction

The intent of these guidelines is to bring a risk-based approach to the application of the security measures throughout the pipeline industry. As stated in the National Infrastructure Protection Plan, DHS assesses risk as a function of threats, vulnerabilities, and consequences. With this in mind, the most effective security programs employ a risk management process that facilitates proactive planning and decision making to mitigate risks for pipeline assets. General steps include:

- Criticality assessments (determine facility criticality);
- Threat assessments (identify known or potential adversaries);
- Vulnerability assessments (identify security weaknesses);
- Risk assessments (based on threat, vulnerability, and criticality assessment findings);
- Risk mitigation (determine and implement appropriate risk reduction countermeasures); and
- Ongoing risk management (monitor, reassess, and modify the program).

Recognizing that there are multiple risk assessment methodologies, each operator should determine the process and methodology most appropriate for implementation of their corporate security plan and the facilities comprising their pipeline system. The operator's risk assessment methodology is subject to review by TSA.

4.2 Criticality Assessment

Determining facility criticality is an essential first step in the security risk management process. Information and findings gathered in the criticality assessment assist operators with prioritizing assets and implementing risk reduction countermeasures. Operators should evaluate each operating facility within their system using the criteria outlined in Section 5.2 to determine or validate criticality. Operators should:

- Conduct facility criticality assessments on a periodic basis, not to exceed 18 months, for all facilities;
- Document the methodology used, and retain the criticality assessment until no longer valid;
- Conduct an SVA or the equivalent as outlined in Section 4.3 of this document for facilities determined to be critical; and
- Maintain and secure the company's list of critical facilities.

The operator's list of critical facilities is subject to review and evaluation by TSA. Operators and TSA will work together towards concurrence on the facilities listed.

4.3 Security Vulnerability Assessment

A security vulnerability assessment is one of the risk assessment methodologies pipeline operators may choose. The SVA serves as a planning and decision support tool to assist security managers with identifying, evaluating, and prioritizing risks; and determining effective security measures to mitigate threats and vulnerabilities to their critical facilities. Common steps performed while conducting an SVA include:

- Asset Characterization - identification of hazards and consequences of concern for the facility, its surroundings, and its supporting infrastructure; and identification of existing layers of protection;
- Threats Assessment - description of possible internal and external threats;
- Security Vulnerability Analysis - identification of potential security vulnerabilities and existing countermeasures and their level of effectiveness in reducing identified vulnerabilities;
- Risk Assessment - determination of the relative degree of risk to the facility in terms of the expected effect on each asset and the likelihood of a success of an attack; and
- Countermeasures Analysis - strategies that reduce the probability of a successful attack or reduce the possible degree of success, strategies that enhance the degree of risk reduction, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

Pipeline operators of critical facilities should:

- Conduct an SVA or the equivalent on a periodic basis, not to exceed 36 months, and within 12 months after completion of a significant enhancement or modification to the facility;
- Document findings from each assessment and retain until no longer valid;
- Implement appropriate findings from the SVA in a timely fashion but no later than 18 months after SVA completion; and
- Document the methodology used and make the documentation available for TSA review upon request.

5 CRITICALITY

5.1 Introduction

The objective in determining which pipeline facilities are critical is to ensure that reasonable and appropriate security risk reduction measures are implemented to protect the most vital assets throughout the pipeline industry.

5.2 Facility Criticality

Given the diverse operational and market settings within which the pipeline industry exists, applying a definition of critical to the nation's pipeline infrastructure presents a significant challenge.

To the maximum extent possible, the approach these guidelines take regarding the determination of pipeline facility criticality is to acknowledge that no entity is more familiar with and able to judge the importance of industry assets than the operator of the facility. However it is necessary for operators to determine the criticality of their facilities using consistent criteria.

Pipeline facilities meeting one or more of the criteria below are considered to be critical:

A facility or combination of facilities that, if damaged or destroyed, would have the potential to:

- Disrupt or significantly reduce required service or deliverability to installations identified as critical to national defense;
- Disrupt or significantly reduce required service or deliverability to key infrastructure (such as power plants or major airports) resulting in major economic disruption;
- Cause mass casualties or significant health effects;
- Disrupt or significantly reduce required service or deliverability resulting in a state or local government's inability to provide essential public services and emergency response for an extended period of time;
- Significantly damage or destroy national landmarks or monuments;
- Disrupt or significantly reduce the intended usage of major rivers, lakes, or waterways. (for example, public drinking water for large populations or disruption of major commerce or public transportation routes);
- Disrupt or significantly reduce required service or deliverability to a significant number of customers or individuals for an extended period of time;
- Significantly disrupt pipeline system operations for an extended period of time, i.e., business critical facilities.

Figure 2 is provided to illustrate the facility criticality determination pathway.

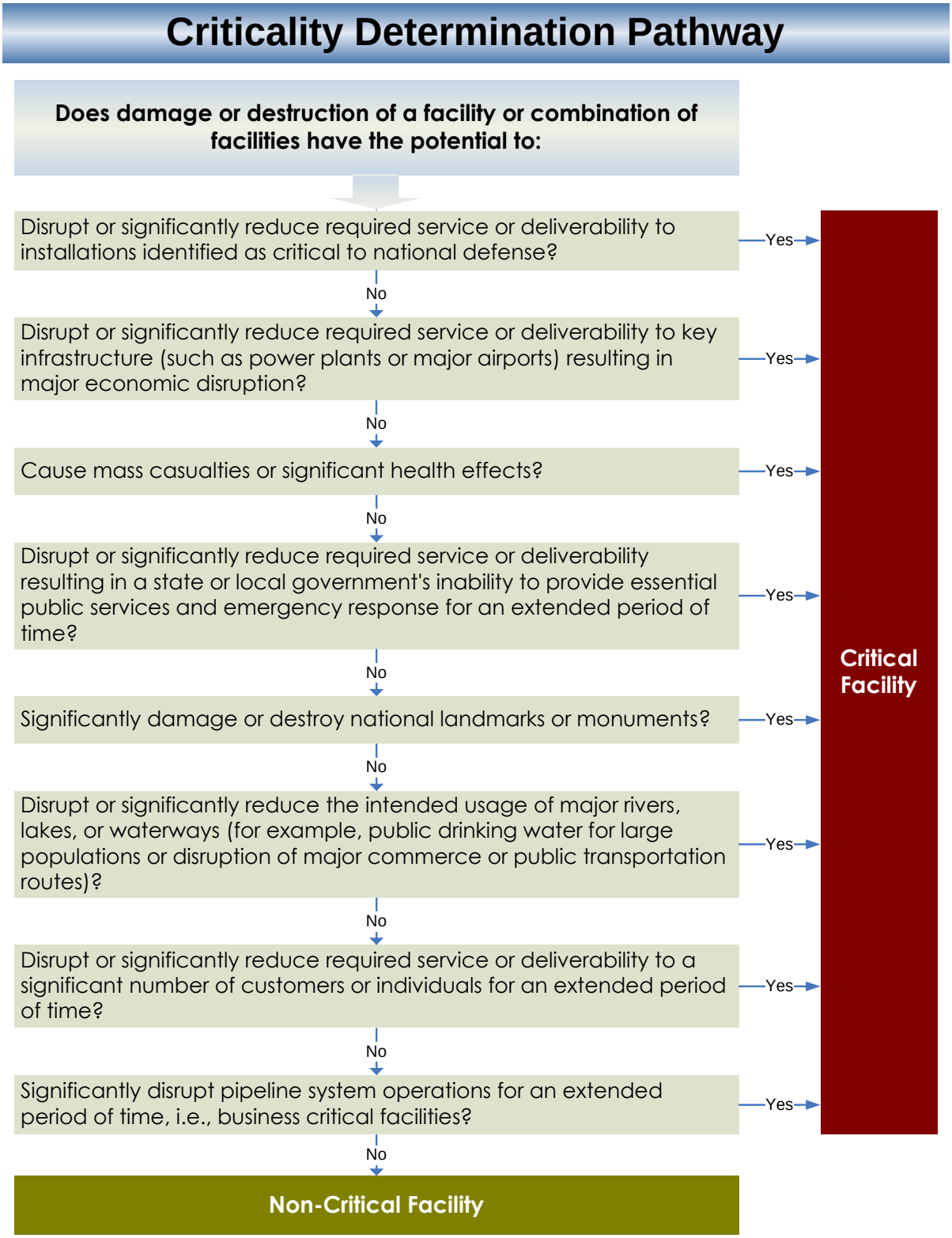

Figure 2: Facility Criticality Determination

6 FACILITY SECURITY MEASURES

6.1 Introduction

Upon completion of the risk analysis process, operators should determine the appropriate mitigation measures for their assets. Section 6.2 provides recommended measures for both critical and non-critical facilities. Recurring program actions are summarized in Appendix A.

6.2 Baseline and Enhanced Security Measures

Pipeline operators should implement baseline security measures at all of their facilities.

Operators should implement **both** baseline and enhanced security measures at each of their critical facilities.

Table 1 identifies the baseline and enhanced security measures for operators to implement at appropriate pipeline facilities.

6.3 Site-Specific Security Measures

Operators should develop, document, and implement site-specific security measures for each of their critical facilities. These measures should be tailored explicitly for each individual facility, with emphasis on specific procedures and actions to be taken at different HSAS threat levels. On a periodic basis, not to exceed 18 months, these facility specific measures should be reviewed and updated as necessary.

Table 1: Baseline and Enhanced Security Measures

	Baseline Security Measures	Enhanced Security Measures
Physical Security and Access Controls	**Barriers**	
	Maintain fences, if used, without gaps around gates or underneath the fence line. Ensure that there is a clear zone for several feet on either side of the fence, free of obstructions, vegetation, or objects that could be used to scale the fence.	Create a security perimeter that deters unauthorized vehicles and persons from entering the facility perimeter or critical areas by installing and maintaining barriers (for example, fences, bollards, jersey barriers, or equivalent.)
	Employ measures to deter unauthorized vehicles and persons from penetrating facility perimeters.	
	Access Controls	
	Employ measures to deter unauthorized persons from gaining access to a facility and restricted areas within a facility.	Implement procedures (such as manual and electronic sign in/out) for controlling access to the facility and restricted buildings or areas within the facility (for example, visitors, contractors, or employees.)
	Close and secure doors, gates, or entrances when not in use.	Monitor and escort visitors at critical facilities.
	Post "No Trespassing" or "Authorized Personnel Only" signs at intervals that are visible from any point of potential entry.	
	Gates	
		Install and maintain gates of an equivalent quality to the barrier to which they are attached.
	Locks and Key Control	
		Establish and document key control procedures for key tracking, issuance, collection, and loss.
		Use patent keys to prevent unauthorized duplication.
		Conduct key inventories every 24 months.
	Facility Lighting	
		Provide sufficient illumination for human or technological recognition of intrusion.
	Intrusion Detection & Monitoring	
		Equip critical facilities or critical areas within a facility with 24/7 monitoring capability to detect and assess unauthorized access.

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Personnel Security	**Personnel Identification and Badging**	
	Develop identification and badging policies and procedures for employees and on-site personnel who have access to secure areas or sensitive information. These policies should address: • Lost or stolen identification cards or badges; • Termination; and • Temporary badges.	Ensure that company or vendor identification is visibly displayed by employees and contractors while on-site.
		Ensure employee and contractor identification cards or badges are secure from tampering and contain the individual's photograph and name.
	Background Investigation	
	Establish policies and procedures for applicant pre-employment screening and behavioral criteria for disqualification of applicants and employees.	Conduct pre-employment background investigations of applicants for positions that are: • Authorized regular unescorted access to control systems or sensitive areas; • Authorized access to sensitive information; • Assigned security roles; • Assigned to work at or granted access rights to critical facilities. At a minimum, investigations should: • Verify and validate identity; • Check criminal history*; and • Verify and validate legal authorization to work. * NOTE: Operators should consider using the Federally-established list of disqualifying crimes applicable to transportation workers at ports (see 49 CFR 1572.103) to assess the suitability of their employees and contractors for these positions.
		Verify that contractors have background investigation policies and procedures at least as rigorous as the pipeline operator's.

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
		Conduct recurring background investigations on a regular basis, not to exceed 10 years, for employees occupying security positions or who have access to sensitive information or areas.
Equipment Maintenance and Testing	**Equipment Maintenance and Testing**	
	Develop and implement a maintenance program to ensure security systems are in good working order.	Verify the proper operation and/or condition of all security equipment on a quarterly basis.
	Identify and respond to security equipment malfunctions or failures in a timely manner.	Conduct an annual inventory of security equipment.
		Provide alternate power sources (for example, generators or battery back-up) or equivalent equipment to minimize interruption of security equipment operation.
Design & Construction	**Design and Construction**	
	Integrate security measures during the design, construction, or renovation of a facility.	Update the facility SVA within 12 months following significant modifications.
Communication	**Communication**	
	Develop internal and external notification requirements and procedures for security events.	Ensure primary and alternate communication capabilities exist for internal and external reporting of all appropriate security events and information.
	Document and periodically update contact (who) and communication (how) information for Federal, state, and local homeland security/law enforcement agencies. (See Appendix B for TSA contact information.)	Establish a defined process for receiving, handling, disseminating, and storing security and threat information.
Personnel Training	**Personnel Training**	
	Provide security awareness briefings for all employees and contractors with unescorted access upon hire and every 2 years thereafter.	Provide security training, to include incident response training, to all full-time, part-time, and contract employees assigned security duties upon hire and annually thereafter.
	Document and maintain records for all security training in accordance with company record retention policy.	

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Exercises & Drills	**Exercises and Drills**	
	Conduct periodic security drills or exercises, to include unannounced tests of security and incident plans. These can be conducted in conjunction with other required drills or exercises.	Conduct or participate in an annual security drill or exercise.
	Develop and implement a written post-exercise report assessing security exercises and documenting corrective actions.	
Security Incident Procedures	**Security Incident Procedures**	
	Implement procedures for responding to security incidents or emergencies and to changes to Homeland Security Alert System (HSAS) levels. These procedures should include the appropriate reporting requirements.	
Recordkeeping	**Recordkeeping**	
	Develop and document recordkeeping policies and procedures for security information. Protection of Sensitive Security Information (SSI) in accordance with the provisions of 49 CFR part 1520 should be specifically addressed.	
	At a minimum, the following documents, as appropriate, should be retained until superseded or replaced: • Corporate Security Plan; • Criticality assessment(s); • Training records; • Exercise reports; • Incident response plan(s); • Security testing and audits; • Security equipment maintenance and testing records. Make security information records available to TSA upon request.	In addition to the documents specified for non-critical facilities, the following documents, applicable to critical facilities, should be retained until superseded or replaced: • SVA(s); • Site-specific measures. Make security information records available to TSA upon request.

7 CYBER ASSET SECURITY MEASURES

7.1 Introduction

The control systems used by operators to manage their infrastructure and products are vital to the pipeline's safe and efficient operation. The growing convergence of information technology (IT) and control systems brings with it increased capabilities, but also increased exposure to cyber attacks against infrastructure. Developing and implementing appropriate security measures reduces the risk to control systems. In the case of legacy components with few or no security features, compensatory controls should be applied as part of an overall defense-in-depth approach.

In this section, the term "system" refers to interconnected hardware and software components, comprising computers, databases, applications, and control and monitoring devices that together perform a particular function or interrelated set of functions. The term "control systems" refers to Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

To implement an effective cyber security strategy, pipeline operators should take advantage of industry and government efforts to develop methodologies, industry standards, and best practices for securing control systems. A list of planning and implementation guidance is provided in Section 7.4.

7.2 Critical Cyber Assets Identification

Operators should evaluate cyber assets and classify them using the following criteria:

- Pipeline control system cyber assets that are essential to safety and/or reliability objectives are classified as critical cyber assets. Baseline and enhanced security measures should be applied to these assets.
- Pipeline control system cyber assets that are not essential to safety and/or reliability objectives are classified as non-critical cyber assets for the purposes of this guideline. Baseline security measures should be applied to these assets.

7.3 Security Measures for Cyber Assets

Table 2 shows the baseline and enhanced cyber security measures that pipeline operators should apply to cyber assets based on their criticality designation.

Table 2: Baseline and Enhanced Cyber Security Measures

BASELINE CYBER SECURITY MEASURES The baseline measures should be applied to all pipeline control system cyber assets.	
General Cyber Security Measures	Provide physical security and access controls to cyber assets.
	Monitor and periodically review, not to exceed 18 months, network connections, including remote and third party connections.
	Evaluate and assess the role of wireless networking for risk before implementation.
	Review and reassess all cyber security procedures annually. Update as necessary.
	Review and reassess cyber asset criticality periodically, not to exceed 18 months.
Information Security Coordination and Responsibilities	Develop a cross-functional cyber security team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks.
	Define information and cyber security roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.
	Establish and document standards for cyber security controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle.
System Lifecycle	Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the SCADA control system architecture is critical for the creation of a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software.
	Establish and document policies and procedures for assessing and maintaining system status and configuration information, for tracking changes made to the control systems network, and for patching and upgrading operating systems and applications.
	Establish and document policies and procedures for the secure disposal of equipment and associated media.
System Restoration & Recovery	Plan and prepare for the restoration and recovery of control systems in a timely fashion as specified in the operator's recovery procedures.

BASELINE CYBER SECURITY MEASURES The baseline measures should be applied to all pipeline control system cyber assets.	
Intrusion Detection & Response	Establish policies and procedures for cyber intrusion monitoring, detection, incident handling, and reporting.
Training	Provide training in information security awareness for all users of control systems before permitting access to the control systems and on an annual basis or as necessitated by changes in the control system. Individuals with significant control systems security roles should have training specific to their roles.
Access Control and Functional Segregation	Segregate and protect the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies both to wired and wireless networks.
	Use control systems hosts and workstations only for approved control system activities.
	Establish and enforce access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks.
ENHANCED CYBER SECURITY MEASURES In addition to baseline measures, operators should apply enhanced measures to all cyber assets that have been designated critical.	
Access Control	Restrict physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, passwords, communications gateways, access control lists, authenticators, and separation of duties, invocation of least privilege, and/or other mechanisms and practices.
	Conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Evaluate the need for enhanced networking control technologies for wireless networks prior to implementation.
Vulnerability Assessment	Conduct periodic vulnerability assessments of the control system security, including testing as appropriate in a non-production environment, not to exceed 36 months.

7.4 Cyber Security Planning and Implementation Guidance

The following is a list of planning and implementation guidance developed by industry and government entities:

- American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*
- American Gas Association (AGA) Report Number 12, *Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*
- American National Standards Institute (ANSI)/International Society of Automation (ISA) – 99.00.01 – 2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*
- ANSI/ISA – 99.02.01 – 2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control System Security Program*
- American Petroleum Institute (API) Standard 1164 *Pipeline SCADA Security*
- U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*
- U.S. Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*

Because of ongoing technological changes, operators should consult these and other cyber security references on a frequent basis in developing and reviewing their company's security measures.

8 HOMELAND SECURITY ADVISORY SYSTEM (HSAS) THREAT LEVEL PROTECTIVE MEASURES

The Homeland Security Advisory System (HSAS) was established by Homeland Security Presidential Directive 3 in March 2002. This five level color-coded system provides a framework to disseminate information regarding the risk of terrorist acts to the nation.

TSA has developed a supplement to this document containing a series of progressive security measures to reduce vulnerabilities to pipeline systems and facilities during periods of heightened threat conditions and to establish a consistent security posture within the pipeline industry. This supplement is unclassified but sensitive and is marked as Sensitive Security Information (SSI). The password-protected document may be obtained by email request to pipelinesecurity@dhs.gov.

APPENDIX A – RECURRING ACTIONS

RECURRING ACTIONS					
	12 Months	**18 Months**	**24 Months**	**36 Months**	**Other**
Baseline	Perform an annual review of the corporate security plan and update as required. (Security Plan, p.5)	Conduct / update facility criticality assessments on a periodic basis, not to exceed 18 months. (Criticality Assessments, p.7)	Provide security awareness briefings for all employees and contractors every two years. (Personnel Training, p.14)		Periodically update contact and communications information for government agencies. (Communications, p.14)
	Review and assess all cyber security procedures annually. (Baseline Cyber Security Measures, p.17)	Review network connections periodically, not to exceed 18 months. (Baseline Cyber Security Measures, p.17)			Conduct security drills and exercises on a periodic basis. (Exercises and Drills, p.15)
	Conduct annual information security and control system security training for appropriate personnel. (Training, p.18)	Review cyber asset criticality periodically, not to exceed 18 months. (Baseline Cyber Security Measures, p.17)			
Enhanced	Conduct a SVA within 12 months of significant modification to a critical facility. (Security Vulnerability Assessment, p.8)	Implement appropriate findings NLT 18 months after SVA completion. (Security Vulnerability Assessment, p.8)	Conduct key inventories every 24 months. (Locks and Key Control, p.12)	Conduct periodic SVAs, not to exceed 36 months. (Security Vulnerability Assessment, p.8)	Conduct recurring background investigations, not to exceed 10 years, for employees in sensitive positions. (Background Investigation, p.14)
	Conduct annual security equipment inventories. (Equipment Maintenance and Testing, p.14)	Review site-specific security measures periodically, not to exceed 18 months. (Facility Security Measures, p. 11)		Conduct control system vulnerability assessments, not to exceed 36 months. (Vulnerability Assessment, p.18)	Verify the proper operation and/or condition of all security equipment on a quarterly basis. (Equipment Maintenance and Testing, p.14)
	Provide annual security training to all security employees. (Personnel Training, p.14)				
	Conduct or participate in an annual security drill or exercise. (Exercises and Drills, p.15)				

Note: 1. Baseline measures apply to all pipeline operators. Enhanced measures apply to operators' critical facilities.
2. All baseline and enhanced security measures are detailed in Section 6 of this document.

APPENDIX B - TSA NOTIFICATION CRITERIA

As the lead Federal agency for pipeline security, TSA desires to be notified of all incidents which are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. Pipeline operators should notify the Transportation Security Operation Center (TSOC) via phone at 866-615-5150 or email at TSOC.ST@dhs.gov as soon as possible if any of the following incidents occurs or if there is other reason to believe that a terrorist incident may be planned or may have occurred:

- Explosions or fires of a suspicious nature affecting pipeline systems, facilities, or assets
- Actual or suspected attacks on pipeline systems, facilities, or assets
- Bomb threats or weapons of mass destruction (WMD) threats to pipeline systems, facilities, or assets
- Theft of pipeline company vehicles, uniforms, or employee credentials
- Suspicious persons or vehicles around pipeline systems, facilities, assets, or right-of-way
- Suspicious photography or possible surveillance of pipeline systems, facilities, or assets
- Suspicious phone calls from people asking about pipeline system, facility, or asset operations, vulnerabilities, or security practices
- Suspicious individuals applying for security-sensitive positions in the pipeline company
- Theft or loss of sensitive security information (detailed pipeline maps, security plans, etc.)
- Actual or suspected cyber attacks that could impact pipeline SCADA or enterprise associated IT systems

When contacting the TSOC, provide as much of the following information as possible:

- Name and contact information
- The time and location of the incident, as specifically as possible
- A description of the incident or activity involved
- Who has been notified and what actions have been taken
- The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate

For questions or concerns, email TSA Pipeline Security Division at pipelinesecurity@dhs.gov

APPENDIX C – LIST OF ACRONYMS

AGA	American Gas Association
ANSI	American National Standards Institute
APGA	American Public Gas Association
API	American Petroleum Institute
CFR	Code of Federal Regulations
DCS	Distributed Control System
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
FEMA	Federal Emergency Management Agency
HSAS	Homeland Security Advisory System
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
ICS	Industrial Control System
INGAA	Interstate Natural Gas Association of America
ISA	International Society of Automation
IT	Information Technology
NIST	National Institute of Standards and Technology
NPRA	National Petrochemical and Refiners Association
PCS	Process Control System
SCADA	Supervisory Control and Data Acquisition
SSI	Sensitive Security Information
SVA	Security Vulnerability Assessment
TIH	Toxic Inhalation Hazard
TSA	Transportation Security Administration
TSNM	Transportation Sector Network Management
TSOC	Transportation Security Operations Center
WMD	Weapons of Mass Destruction

APPENDIX D – REFERENCE DOCUMENTS

Operators should consult the current edition of these and other security references on a frequent basis in developing and reviewing their company's security program.

American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*

American Gas Association (AGA), Interstate Natural Gas Association of America (INGAA) & American Public Gas Association (APGA), *Security Guidelines: Natural Gas Industry, Transmission and Distribution*

AGA Report Number 12, *Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*

American National Standards Institute (ANSI)/International Society of Automation (ISA) – 99.00.01 – 2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*

ANSI/ISA – 99.02.01 – 2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control System Security Program*

American Petroleum Institute (API) & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*

API Standard 1164, *Pipeline SCADA Security*

API, *Security Guidelines for the Petroleum Industry*

Homeland Security Presidential Directive 3: *Homeland Security Advisory System*

Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection.*

U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*

U.S. Department of Homeland Security, Federal Emergency Management Agency (FEMA), *Homeland Security Exercise and Evaluation Program (HSEEP) Vols. 1 - 4*

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*

U.S. Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*

U.S. Department of Homeland Security, Transportation Security Administration (TSA), *Pipeline Security Smart Practices*

U.S. Department of Homeland Security, TSA, *Transportation Systems Sector-Specific Plan: Pipeline Modal Annex*

This page intentionally left blank.