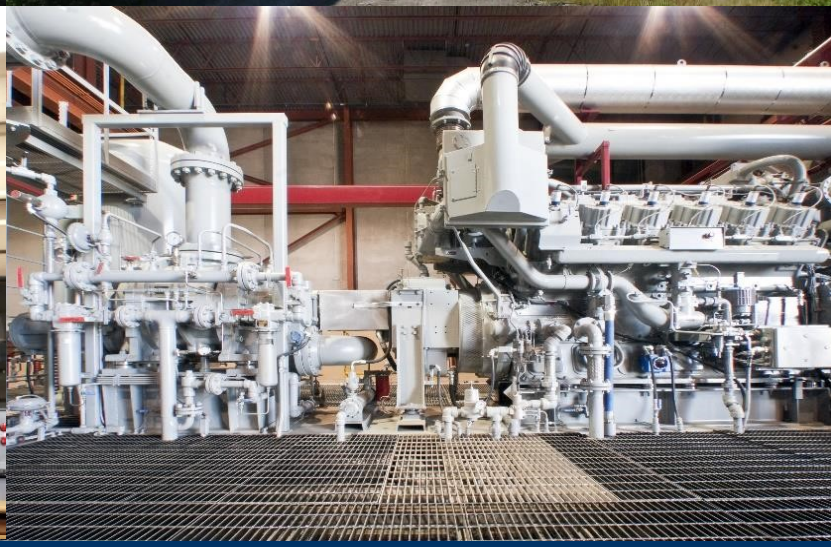


Pipeline Security Guidelines

March 2018

Transportation Security Administration

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." On September 8, 2002, TSA initiated its pipeline security efforts. Those responsibilities now reside within the Office of Security Policy and Industry Engagement's Surface Division.

1.1 Background and Purpose

In executing its responsibility for national pipeline security, TSA originally 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. The 2010 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 was soon revised resulting in the 2011 Pipeline Security Guidelines.

The advancement of security practices to meet the ever changing threat environment in both the physical and cyber security realms required that the guidelines be updated again. Utilizing a similar industry and government collaborative approach, TSA developed this document, which supersedes the 2011 version of the Pipeline Security Guidelines.

The security measures in this guidance provide the basis for TSA's Pipeline Security Program Corporate Security Reviews and Critical Facility Security Reviews. This document is guidance and does not impose requirements on any person or company. The term "should" means that TSA recommends the actions described. Nothing in this document shall supersede Federal statutory or regulatory requirements.

1.2 Scope

These guidelines are applicable to operational natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility operators. Additionally, they apply to operational 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.

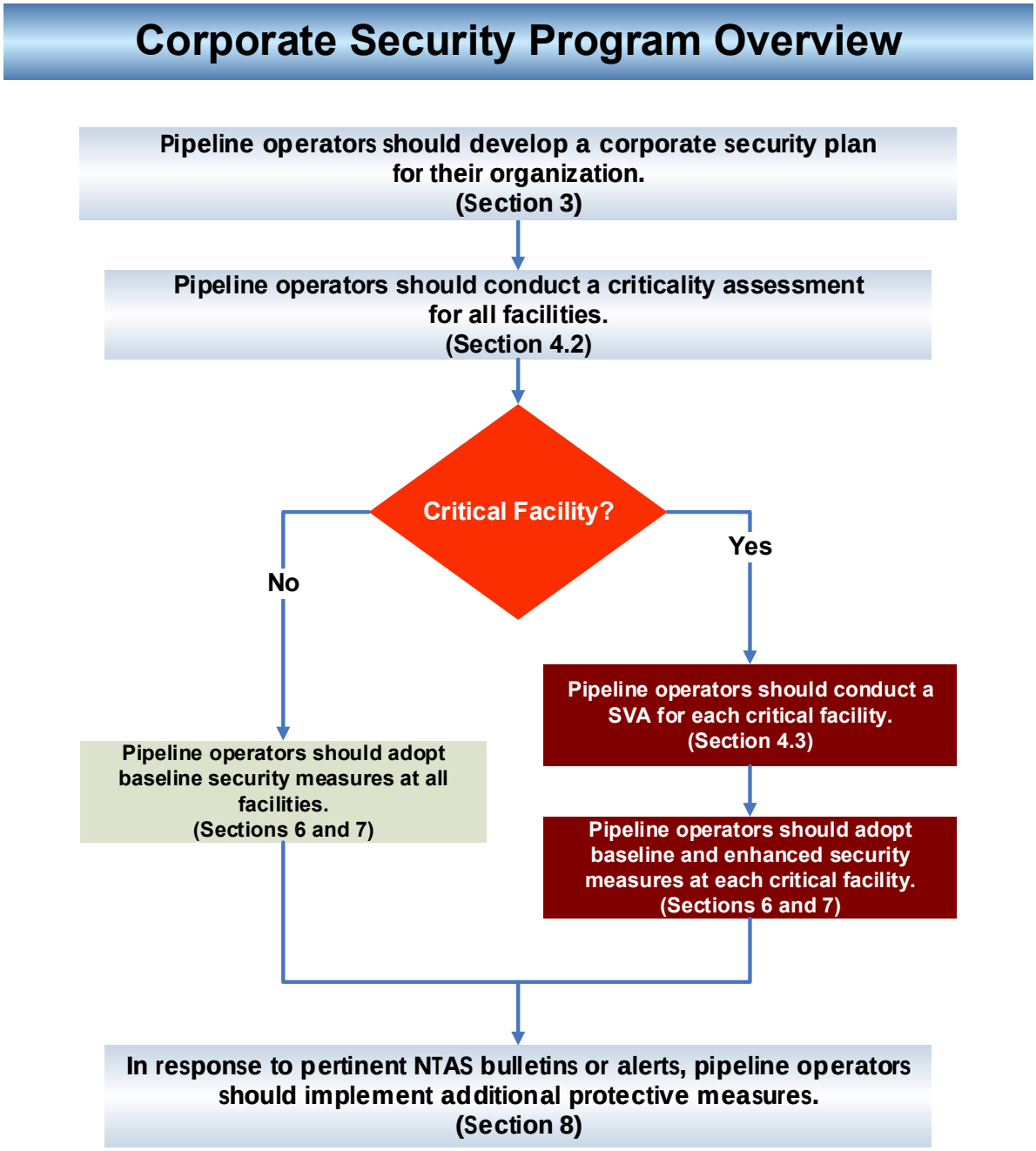
2 CORPORATE SECURITY PROGRAM

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:

- Develop a corporate security plan as described in Section 3;
- Ensure sufficient resources, to include trained staff and equipment, are provided to effectively execute the corporate security program;
- Ensure identified security deficiencies have appropriate financial resources allocated in the corporate budgeting and purchasing processes;
- Assign a qualified primary and alternate staff member to manage the corporate security program;
- 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;
- Implement appropriate threat level protective measures upon receipt of a pertinent National Terrorism Advisory System (NTAS) Bulletin or Alert; and
- Notify TSA of security incidents meeting the criteria provided in Appendix B by phone or email as soon as possible.

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 policies and procedures, to include, but not limited to, methodologies used and timelines established for conducting criticality assessments, risk assessments, and security vulnerability assessments (SVAs), if applicable;
- Reference other company plans, policies and procedures such as insider threat, business continuity, incident response and recovery plans;
- Be reviewed on an annual basis, and updated as required based on findings from assessments, major 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 provided to TSA for review 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.

- **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 personnel, facilities, off-site responders, and procedures for notification of government and law enforcement agencies.
- **Personnel Training** - Describe security training requirements, to include training in security equipment operation, security awareness, and security incident recognition and reporting procedures for company personnel and contractors.
- **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.
- **NTAS Response Procedures** - Describe the operator's additional protective measures for periods of heightened threat corresponding to the duration of Department of Homeland Security (DHS) NTAS Bulletins or Alerts.
- **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, SVAs, and other company sensitive security information, 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 auditing and testing of the effectiveness of the company's security plan and procedures, to include documentation of results.
- **Outreach** - Describe policies and procedures for company security awareness outreach efforts to neighbors, law enforcement, media, and the public.

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 planning and decision making to mitigate risks for pipeline assets. General elements include:

- Assessments used to determine facility criticality;
- Threat assessments identifying known or potential adversaries;
- Vulnerability assessments identifying security weaknesses;
- Risk assessments (based on threat, vulnerability, and consequence, considering facility criticality assessment findings);
- Risk mitigation to determine and implement appropriate risk reduction countermeasures; and
- Ongoing risk management to 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 the corporate security plan at the facilities comprising their pipeline system. TSA may ask to review the operator's risk assessment methodology.

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

- 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 success of an attack; and
- Countermeasures Analysis – comparison of 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.

Operators of critical pipeline 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;
- Conduct an SVA or the equivalent for newly identified or constructed critical facilities within 12 months of designation or after achieving operational status.
- Document findings from each assessment and retain them until no longer valid;
- Implement appropriate findings from the SVA in a timely fashion but no later than 24 months after SVA completion; and
- Document the assessment 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

Identifying the critical components of the nation's pipeline infrastructure is a significant challenge considering the diverse operational and market environment of the pipeline industry. Pipeline system operators are uniquely positioned to understand the criticality of their facilities. However, it is appropriate for operators to determine the criticality of their facilities using consistent criteria.

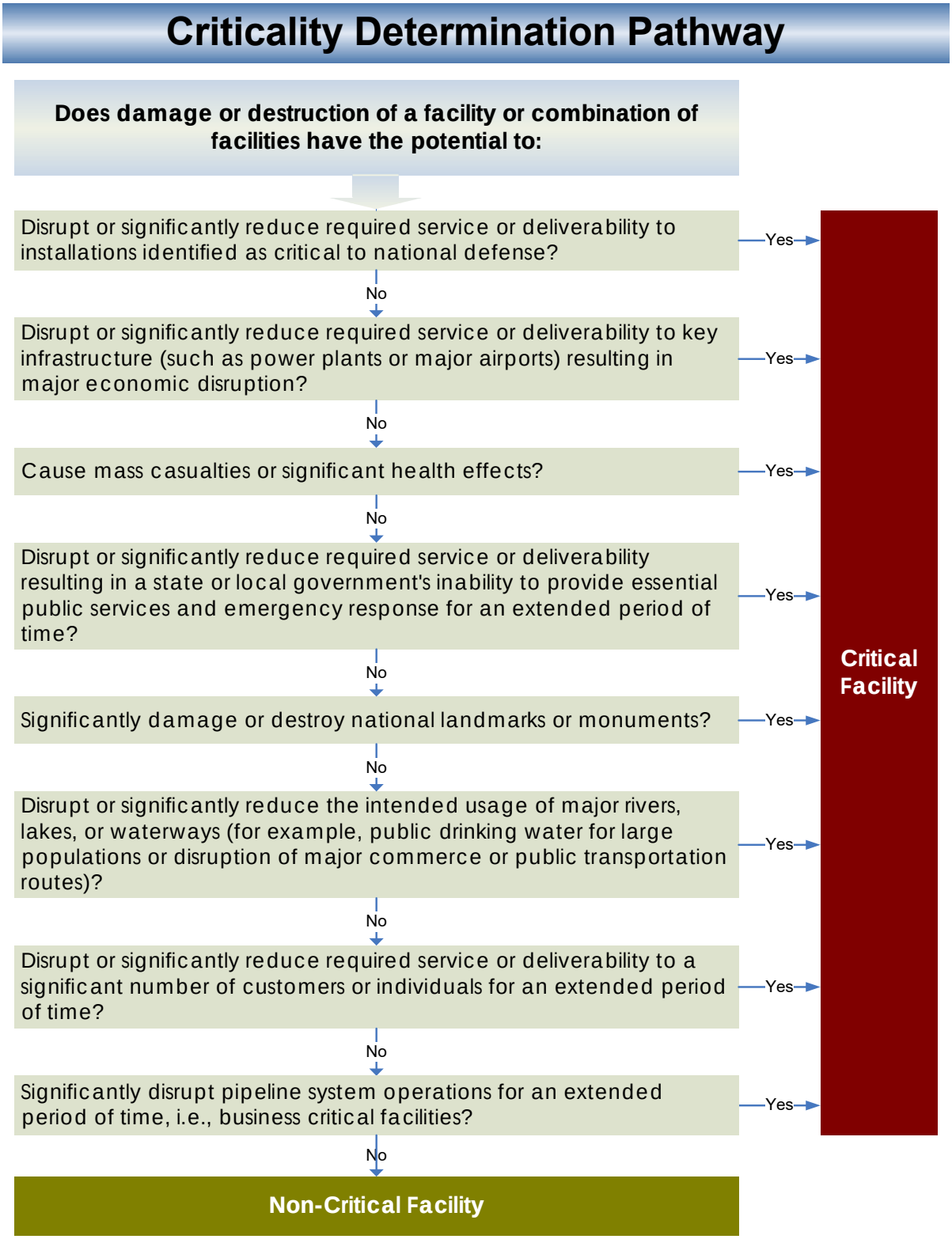
Pipeline facilities meeting any one or more of the criteria below are considered to be critical:

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 use of major rivers, lakes, or waterways. (e.g., 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.

Factors such as customer base, downstream deliverability and reliability commitments, system redundancies, and operator risk tolerance may influence critical determinations. 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 both critical and non-critical facilities.

6.2 Baseline and Enhanced Security Measures

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

Operators should develop and 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. Recurring actions are summarized in Appendix A.

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 facility and address specific actions to be taken in response to pertinent NTAS Bulletins or Alerts. On a periodic basis, not to exceed 18 months, these site-specific security 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 Control	**Fencing / Barriers**	
	Employ measures to impede unauthorized access to facilities.	Create a security perimeter that impedes unauthorized vehicles from entering the facility perimeter or critical areas by installing and maintaining barriers (e.g., fences, bollards, jersey barriers, or equivalent.)
	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 for concealment or to scale the fence.	
	Access Controls	
	Employ measures to impede unauthorized persons from gaining access to a facility and restricted areas within a facility.	Implement procedures (such as manual or electronic sign in/out) for controlling access to the facility and restricted buildings or areas within the facility.
	Close and secure perimeter 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 issuance, tracking, collection, loss, and unauthorized duplication.
		Use patent keys to prevent unauthorized duplication.
		Conduct key inventories every 24 months.

Table 1: Baseline and Enhanced Security Measures

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Physical Security and Access Control	**Facility Lighting**	
		Provide sufficient illumination for human or technological recognition of intrusion into the facility perimeter or critical areas.
	Intrusion Detection & Monitoring	
		Provide critical facilities or critical areas within a facility with security measures to monitor, detect, and assess unauthorized access 24 hours a day, 7 days a week.
Personnel Security	**Personnel Identification and Badging**	
	Develop identification and badging policies and procedures for personnel who have access to secure areas or sensitive information. These policies should address: • Lost or stolen identification cards or badges; • Temporary badges; and • Personnel termination.	Ensure that company or vendor identification is available for examination by being visibly displayed or carried by personnel while on-site.
		Ensure personnel 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 (see 49 CFR 1572.103) to assess the suitability of their personnel for these positions.

Table 1: Baseline and Enhanced Security Measures

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Personnel Security		Verify that contractors have background investigation policies and procedures at least as rigorous as the pipeline operator's.
		Conduct recurring background investigations on a regular basis (as labor laws or bargaining unit contracts allow), 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.	Through routine use or quarterly examination, verify the proper operation and/or condition of all security equipment.
	Identify and respond to security equipment malfunctions or failures in a timely manner.	
		Provide an equivalent level of protective security measures to mitigate risk during power outages, security equipment failure, or extended repair of security systems.
Design & Construction	**Design and Construction**	
	Integrate security risk mitigation measures during the design, construction, or renovation of a facility.	Conduct an SVA for newly identified or constructed critical facilities within 12 months of designation or after achieving operational status.
		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 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.

Table 1: Baseline and Enhanced Security Measures

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Personnel Training	**Personnel Training**	
	Provide security awareness briefings, to include security incident recognition and reporting procedures, for personnel with unescorted access upon hiring and every 3 years thereafter.	Provide security training, to include incident response training, to personnel-assigned security duties upon hiring and annually thereafter.
	Document security training and maintain records in accordance with company record retention policy.	
Drills and Exercises	**Drills and Exercises**	
	Conduct periodic security drills or exercises, to include announced or unannounced tests of security and incident plans. These can be conducted in conjunction with other required drills or exercises. * NOTE: Response to an actual security incident can satisfy this measure.	Conduct or participate in an annual security drill or exercise. Multiple facilities may participate in a common drill or exercise.
		Develop and implement a written post-event report assessing security drills or exercises and documenting corrective actions.
Security Incident Procedures	**Security Incident Procedures**	
	Implement procedures for responding to security incidents or emergencies and to pertinent National Terrorism Advisory System (NTAS) Bulletins or Alerts. These procedures should include the appropriate reporting requirements.	
	Post bomb threat checklists by telephones at staffed facilities.	

Table 1: Baseline and Enhanced Security Measures

	BASELINE SECURITY MEASURES	ENHANCED SECURITY MEASURES
Recordkeeping	**Recordkeeping**	
	Develop and document recordkeeping policies and procedures for security information. Protection of SSI in accordance with the provisions of 49 CFR Parts 15 and 1520 should be specifically addressed.	
	The following documents, as appropriate, should be retained until superseded or replaced: • Corporate Security Plan; • Criticality assessment(s); • Training records; • Security drill or exercise reports; • Incident response plan(s); • Security testing and audits. 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.
Outreach	**Outreach**	
		Conduct outreach to nearby law enforcement agencies to ensure awareness of the facility's functions and significance.
		Conduct outreach to neighboring businesses to coordinate security efforts. Also conduct outreach to neighboring residences to provide facility security awareness.

7 PIPELINE CYBER ASSET SECURITY MEASURES

7.1 Introduction

The operational technology used by the operators to manage their infrastructure and products are vital to the pipeline system's safe and efficient operation. “Operational technologies” (OT) are the systems that detect or cause a change through the direct monitoring and/or control of physical devices, processes and events in the pipelines. OT systems include control systems (SCADA, process control systems (PCS), distributed control systems (DCS)), measurement systems and telemetry systems, which are collectively referred to as “pipeline cyber assets.”

The National Institute of Standards and Technology (NIST) has developed the *Framework for Improving Critical Infrastructure Cybersecurity,* a set of standards and best practices to assist organizations in managing cybersecurity risks and to promote the protection of critical infrastructure. To implement an effective cybersecurity strategy, pipeline operators should consider the approach outlined in the NIST Framework and the guidance issued by DHS and the Department of Energy along with industry-specific or other established methodologies, standards, and best practices (see Section 7.4).

7.2 Pipeline Cyber Assets Classification

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

- Critical pipeline cyber assets are OT systems that can control operations on the pipeline. Baseline and enhanced security measures should be applied to these assets.
- Non-critical pipeline cyber assets are OT systems that monitor operations on the pipeline. Baseline security measures should be applied to these assets.

7.3 Security Measures for Pipeline Cyber Assets

Table 2 shows the baseline and enhanced cybersecurity measures that pipeline operators should apply to pipeline cyber assets based on their criticality designation. These measures incorporate updates to the previous TSA Pipeline Security Guidelines as well as recommendations and practices from the government and industry documents listed in Section 7.4. The cybersecurity guidelines that follow are organized according to the relevant functions and categories presented in the NIST Framework.

Table 2: Baseline and Enhanced Cyber Security Measures

	Baseline Security Measures	Enhanced Security Measures
Identify	**Asset Management**	
	Establish and document policies and procedures for assessing and maintaining configuration information, for tracking changes made to the pipeline cyber assets, and for patching/upgrading operating systems and applications. Ensure that the changes do not adversely impact existing cybersecurity controls.	Employ mechanisms to maintain accurate inventory and to detect unauthorized components.
	Develop and maintain a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third party connections, and information flows.	Review network connections periodically, including remote and third party connections. Develop a detailed inventory for every endpoint.
	Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months.	
	Business Environment	
	Ensure that any change that adds control operations to a non-critical pipeline cyber asset results in the system being recognized as a critical pipeline cyber asset and enhanced security measures being applied.	
	Governance	
	Establish and distribute cybersecurity policies, plans, processes and supporting procedures commensurate with the current regulatory, risk, legal and operational environment.	
	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 36 months, or when there is a significant organizational or technological change. Update as necessary.	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 12 months, or when there is a significant organizational change. Update as necessary.
	Risk Management Strategy	
	Develop an operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks.	

Table 2: Baseline and Enhanced Cyber Security Measures

	Baseline Security Measures	Enhanced Security Measures
Identify	**Risk Assessment**	
	Establish a process to identify and evaluate vulnerabilities and compensating security controls.	Ensure threat and vulnerability information received from information sharing forums and sources are made available to those responsible for assessing and determining the appropriate course of action.
Protect	**Access Control**	
	Establish and enforce unique accounts for each individual user and administrator, establish security requirements for certain types of privileged accounts, and prohibit the sharing of these accounts. In instances where systems do not support unique user accounts, then implement appropriate compensating security controls (e.g., physical controls).	Restrict user physical access to control systems and control networks through the use of appropriate controls. Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).
	Ensure that user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company.	
	Establish and enforce access control policies for local and remote users. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections.	Monitor physical and remote user access to critical pipeline cyber assets.
	Ensure appropriate segregation of duties is in place. In instances where this is not feasible, apply appropriate compensating security controls.	
	Change all default passwords for new software, hardware, etc., upon installation. In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), implement appropriate compensating security controls (e.g., administrative controls).	Employ mechanisms to support the management of accounts.

Table 2: Baseline and Enhanced Cyber Security Measures

	Baseline Security Measures	Enhanced Security Measures
Protect	**Awareness and Training**	
	Ensure that all persons requiring access to the organization's pipeline cyber assets receive cybersecurity awareness training.	Provide role-based security training on recognizing and reporting potential indicators of system compromise prior to obtaining access to the critical pipeline cyber assets.
	Establish and execute a cyber-threat awareness program for employees. This program should include practical exercises/testing.	
	Data Security & Information Protection	
	Establish and implement policies and procedures to ensure data protection measures are in place, including identifying critical data and establishing classification of different types of data, establishing specific handling procedures, and protections and disposal.	
	Protective Technology	
	Segregate and protect the pipeline cyber assets from enterprise networks and the internet using physical separation, firewalls and other protections.	
	Regularly validate that technical controls comply with the organization's cybersecurity policies, plans and procedures, and report results to senior management.	
	Implement technical or procedural controls to restrict the use of pipeline cyber assets for only approved activities.	
Detect	**Anomalies and Events**	
	Implement processes to generate alerts and log cybersecurity events in response to anomalous activity. Review the logs and respond to alerts in a timely manner.	
	Security Continuous Monitoring	
	Monitor for unauthorized access or the introduction of malicious code or communications.	
	Conduct cyber vulnerability assessments as described in your risk assessment process	Utilize independent assessors to conduct pipeline cyber security assessments.

Table 2: Baseline and Enhanced Cyber Security Measures

	Baseline Security Measures	Enhanced Security Measures
Detect	**Detection Processes**	
	Establish technical or procedural controls for cyber intrusion monitoring and detection.	
	Perform regular testing of intrusion and malware detection processes and procedures.	
Respond	**Response Planning**	
	Establish policies and procedures for cybersecurity incident handling, analysis and reporting, including assignment of the specific roles/tasks to individuals and teams.	Conduct cybersecurity incident response exercises periodically.
	Establish and maintain a cyber-incident response capability.	Establish and maintain a process that supports 24 hours a day cyber incident response.
	Communications	
	Report significant cyber incidents to senior management; appropriate federal, state, local, tribal, and territorial (SLTT) entities; and applicable ISAC(s).	Pipeline operators should follow the notification criteria in Appendix B
	Mitigation	
	Ensure the organization's response plans and procedures include mitigation measures to help prevent further impacts.	
Recover	**Recovery Planning**	
	Establish a plan for the recovery and reconstitution of pipeline cyber assets within a timeframe to align with the organization's safety and business continuity objectives.	
	Improvements	
	Review the organization's cyber recovery plan annually. Update as necessary.	

7.4 Cyber Security Planning and Implementation Guidance

The following is a list of planning and implementation guidance developed by industry or Federal government entities. Operators should consult the current edition of these and other cyber security references on a frequent basis in developing and reviewing their company's cyber security program.

- 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*
- ANSI/API Standard 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*
- U.S. Department of Commerce, National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*
- U.S. Department of Commerce, NIST, Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*
- U.S. Department of Homeland Security, Office of Infrastructure Protection, *Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards,* May 2009
- U.S Department of Energy, Office of Electricity Delivery and Energy Reliability, *Energy Sector Cybersecurity Framework Implementation Guidance,* January 2015
- U.S Department of Homeland Security, *Transportation Systems Sector Cybersecurity Framework Implementation Guidance,* June 2015

8 PROTECTIVE MEASURES FOR NATIONAL TERRORISM ADVISORY SYSTEM (NTAS) ALERTS

The Department of Homeland Security's NTAS provides a framework to disseminate information via Bulletins or Alerts regarding the threat of terrorist acts to the nation.

TSA has developed a supplement to this document containing recommended security measures to reduce vulnerabilities to pipeline systems and facilities during periods of heightened threat 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. (Section 3.1)	Conduct facility criticality assessments on a periodic basis, not to exceed 18 months. (Section 4.2)			Periodically update contact and communications information for government agencies. (Table 1 Communication)
					Conduct security drills or exercises on a periodic basis. (Table 1 Drills and Exercises)
	Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months. (Table 2 Cyber Asset Management)			Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 36 months. (Table 2 Cyber Governance)	Perform regular testing of intrusion and malware detection processes and procedures. (Table 2 Cyber Detection Processes)
	Review the organization's cyber recovery plan annually. (Table 2 Cyber Improvements)				Conduct cybersecurity incident response exercises periodically. (Table 2 Cyber Response Planning)
					Periodically review facility staffing requirements for implementing additional security measures. (NTAS Supplement, p.1)
					Provide notification of a pipeline incident in accordance with Appendix B.

RECURRING ACTIONS					
	12 Months	**18 Months**	**24 Months**	**36 Months**	**Other**
Enhanced	Conduct a SVA within 12 months of significant modification to a critical facility, a newly identified critical facility or a newly constructed facility identified as critical. (Section 4.3)		Implement appropriate findings NLT 24 months after SVA completion. (Section 4.3)	Conduct periodic SVAs, not to exceed 36 months. (Section 4.3)	
		Review site-specific security measures periodically, not to exceed 18 months. (Section 6.3)	Conduct key inventories every 24 months. (Table 1 Locks and Key Control)		Verify the proper operation and/or condition of all security equipment through routine use or quarterly examination. (Table 1 Equipment Maintenance and Testing)
	Conduct or participate in an annual security drill or exercise. (Table 1 Exercises and Drills)				Conduct recurring background investigations, not to exceed 10 years, for employees occupying security positions or in sensitive positions. (Table 1 Background Investigation)
	Provide security training to personnel assigned security duties upon hiring and annually thereafter. (Table 1 Personnel Training)			Provide security awareness briefings for personnel with unescorted access upon hiring and every 3 years thereafter. (Table 1 Personnel Training)	
	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 12 months. (Table 2 Cyber Governance)				

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 requests to be notified of security incidents that are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be considered precursors to such an attempt. Pipeline operators should notify the Transportation Security Operations 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 inquiries 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.).

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;
- Which entities have been notified and what actions have been taken;
- The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate.

Actual or suspected cyber-attacks that could impact pipeline industrial control systems (SCADA, PCS, DCS), measurement systems and telemetry systems or enterprise associated IT systems should be reported to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870.

For questions or concerns, email the TSA Pipeline Security staff 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
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
NTAS	National Terrorism Advisory System
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
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. Cyber planning and implementation guidance appears in Section 7.4.

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

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

API, *Security Guidelines for the Petroleum Industry*

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

Presidential Policy Directive 7: *National Terrorism Advisory System (NTAS)*

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*