October 2004

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

American Petroleum Institute

NPRA

October 2004

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

American Petroleum Institute
1220 L Street, NW
Washington, DC
20005-4070

National Petrochemical &
Refiners Association
1899 L Street, NW
Suite 1000
Washington, DC
20036-3896

PREFACE

The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) are pleased to make this Second Edition of this Security Vulnerability Assessment Methodology available to members of petroleum and petrochemical industries. The information contained herein has been developed in cooperation with government and industry, and is intended to provide a tool to help maintain and strengthen the security of personnel, facilities, and industry operations; thereby enhancing the security of our nation's energy infrastructure.

API and NPRA wish to express sincere appreciation to the member companies who have made personnel available to work on this document. We especially thank the Department of Homeland Security and its Directorate of Information Analysis & Infrastructure Protection and the Department of Energy's Argonne National Laboratory for their invaluable contributions. The lead consultant in developing this methodology has been David Moore of the AcuTech Consulting Group, whose help and experience was instrumental in developing this document. Lastly, we want to acknowledge the contributions of the Centers for Chemical Process Safety for their initial work on assessing security vulnerability in the chemical industry.

This methodology constitutes but one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

The focus of this second edition was to expand the successful first edition by including additional examples of how the methodology can be applied to a wide range of assets and operations. This includes petroleum refining and petrochemical manufacturing operations, pipelines, and transportation including truck and rail. The methodology was originally field tested at two refinery complexes, including an interconnected tank farm, marine terminal and lube plant before the publication of the first edition. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industries.

API and NPRA are not undertaking to meet the duties of employers, manufacturers, or suppliers to train and equip their employees, nor to warn any who might potentially be exposed, concerning security risks and precautions. Ultimately, it is the responsibility of the owner or operator to select and implement the security vulnerability assessment method and depth of analysis that best meet the needs of a specific location.

CONTENTS

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

Chapter 1 Introduction

1.1 INTRODUCTION TO SECURITY VULNERABILITY ASSESSMENT

The first step in the process of managing security risks is to identify and analyze the threats and the vulnerabilities facing a facility by conducting a Security Vulnerability Assessment (SVA). The SVA is a systematic process that evaluates the likelihood that a threat against a facility will be successful. It considers the potential severity of consequences to the facility itself, to the surrounding community and on the energy supply chain.

The SVA process is a team-based approach that combines the multiple skills and knowledge of the various participants to provide a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the SVA team may include individuals with knowledge of physical and cyber security, process safety, facility and process design and operations, emergency response, management and other disciplines as necessary.

The objective of conducting a SVA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company. With this information security risks can be assessed and strategies can be formed to reduce vulnerabilities as required. SVA is a tool to assist management in making decisions on the need for countermeasures to address the threats and vulnerabilities.

1.2 OBJECTIVES, INTENDED AUDIENCE AND SCOPE OF THE GUIDANCE

This document was prepared by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) Security Committees to assist the petroleum and petrochemical industries in understanding security vulnerability assessment and in conducting SVAs. The guidelines describe an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues they face. During the development process it was field tested at two refineries, two tank farms, and a lube plant, which included typical process equipment, storage tanks, marine operations, infrastructure, pipelines, and distribution terminals for truck and rail. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industry.

This methodology constitutes one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the needs of the specific location. Differences in geographic location, type of operations, and on-site quantities of hazardous substances all play a role in determining the level of SVA and the approach taken. Independent of the SVA method used, all techniques include the following activities:

- Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
- Identify potential security vulnerabilities that threaten the asset's service or integrity;
- Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
- Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk;
- Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk to ensure adequate countermeasures are being applied.

This guidance was developed for the industry as an adjunct to other available references which includes:

- American Petroleum Institute, "Security Guidelines for the Petroleum Industry", May, 2003;
- API RP 70, "Security for Offshore Oil and Natural Gas Operations", First Edition, April, 2003;

- "Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites", American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS¨), August, 2002;
- "Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF)", Sandia National Laboratories, 2002.

API and NPRA would like to acknowledge the contribution of the Center for Chemical Process Safety (CCPS) compiled in their "Guidelines for Analyzing and Managing the Security of Fixed Chemical Sites." It was this initial body of work that was used as a basis for developing the first edition of the API NPRA SVA methodology. Although similar in nature, the SVA Method was developed for the petroleum and petrochemical industry, at both fixed and mobile systems. Examples have been added that demonstrate applicability at various operating segments of the industry. Owner/Operators may want to use any of the methods above, or another equivalent and appropriate methodology in conducting their SVAs. These guidelines should also be considered in light of any applicable federal, state and local laws and regulations.

The guidance is intended for site managers, security managers, process safety managers, and others responsible for conducting security vulnerability analyses and managing security at petroleum and petrochemical facilities.

The method described in this guidance may be widely applicable to a full spectrum of security issues, but the key hazards of concern are malevolent acts, such as terrorism, that have the potential for widespread casualties or damage.

These guidelines provide additional industry segment specific guidance to the overall security plan and SVA method presented in Part I of the API Security Guidelines for the Petroleum Industry.

1.3 SECURITY VULNERABILITY ASSESSMENT AND SECURITY MANAGEMENT PRINCIPLES

Owner/Operators should ensure the security of facilities and the protection of the public, the environment, workers, and the continuity of the business through the management of security risks. The premise of the guidelines is that security risks should be managed in a risk-based, performance-oriented management process.

The foundation of the security management approach is the need to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of the countermeasures provided to mitigate the threats. Security Vulnerability Assessment is a management tool that can be used to assist in accomplishing this task, and to help the owner/operator in making decisions on the need for and value of enhancements.

The need for security enhancements will be determined partly by factors such as the degree of the threat, the degree of vulnerability, the possible consequences of an incident, and the attractiveness of the asset to adversaries. In the case of terrorist threats, higher risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of consequences, and where the level of vulnerability and threat is high.

SVAs are not necessarily a quantitative risk assessment, but are usually performed qualitatively using the best judgment of the SVA Team. The expected outcome is a qualitative determination of risk to provide a sound basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

A basic premise is that all security risks cannot be completely prevented. The security objectives are to employ four basic strategies to help minimize the risk:

1. Deter
2. Detect
3. Delay
4. Respond

Appropriate strategies for managing security can vary widely depending on the individual circumstances of the facility, including the type of facility and the threats facing the facility. As a result, this guideline does not prescribe security measures but instead suggests means of identifying, analyzing, and reducing vulnerabilities. The specific situations must be evaluated individually by local management using best judgment of applicable practices. Appropriate security risk management decisions must be made commensurate with the risks. This flexible approach recognizes that there isn't a uniform approach to security in the petroleum industry, and that resources are best applied to mitigate high-risk situations primarily.

All Owner/Operators are encouraged to seek out assistance and coordinate efforts with federal, state, and local law enforcement agencies, and with the local emergency services and Local Emergency Planning Committee. Owner/Operators can also obtain and share intelligence, coordinate training, and tap other resources to help deter attacks and to manage emergencies.

Chapter 2 Security Vulnerability Assessment Concepts

2.1 INTRODUCTION TO SVA TERMS

A Security Vulnerability Assessment (SVA) is the process that includes determining the likelihood of an adversary successfully exploiting vulnerability and estimating the resulting degree of damage or impact. Based on this assessment, judgments can be made on degree of risk and the need for additional countermeasures. To conduct a SVA, key terms and concepts must be understood as explained in this chapter.

2.2 RISK DEFINITION FOR SVA

For the purposes of a SVA, the definition of risk is shown in Figure 2.1. The risk that is being analyzed for the SVA is defined as an expression of the likelihood that a defined threat will target and successfully attack a specific security vulnerability of a particular target or combination of targets to cause a given set of consequences. The complete SVA may evaluate one or more issues or sum the risk of the entire set of security issues. The risk variables are defined as shown in Figure 2.2.

A high-risk event, for example, is one which is represented by a high likelihood of a successful attack against a given critical target asset. Likelihood is determined by considering several factors including its attractiveness to the adversary, the degree of threat, and the degree of vulnerability. Criticality is determined by the asset's importance or value, and the potential consequences if attacked. If the likelihood of a successful attack against an important asset is high, then the risk is considered high and appropriate countermeasures would be required for a critical asset at high risk.

For the SVA, the risk of the security event is normally estimated qualitatively. It is based on the consensus judgment of a team of knowledgeable people as to how the likelihood and consequences of an undesired event scenario compares to other scenarios. The assessment is based on best available information, using experience and expertise of the team to make sound risk management decisions. The team may use a risk matrix, which is a graphical representation of the risk factors, as a tool for risk assessment decisions.

The API NPRA SVA Methodology has a two step screening process to focus attention on higher risk events. The key variables considered in the first screening are Consequences and Target Attractiveness. If either of those are either not sufficiently significant, the asset is screened out from further specific consideration. Later, the complete set of risk variables shown in Figure 2.1 are used in the second screen to determine the need for additional specific countermeasures.

Figure 2.1—Risk Definition

Security Risk is a function of: • **Consequences** of a successful attack against an asset and • **Likelihood** of a successful attack against an asset.
Likelihood is a function of: • the **Attractiveness** to the adversary of the asset, • the degree of **Threat** posed by the adversary, and • the degree of **Vulnerability** of the asset.

Figure 2.2—SVA Risk Variables[4]

Consequences	*Consequences* are the potential adverse impacts to a facility, the local community and/or the nation as a result of a successful attack.
Likelihood	*Likelihood* is a function of the chance of being targeted for attack, and the conditional chance of mounting a successful attack (both planning and executing) given the threat and existing security measures. This is a function of Threat, Vulnerability, and Target Attractiveness (see Figure 2.1).
Attractiveness	*Attractiveness* is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to a specific adversary.
Threat	*Threat* is a function of an adversary's intent, motivation, capabilities, and known patterns of operation. Different adversaries may pose different threats to various assets within a given facility or to different facilities.
Vulnerability	*Vulnerability* is any weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt a critical function. This is a variable that indicates the likelihood of a successful attack given the intent to attack an asset.

[4]Ibid, AIChE.

2.3 CONSEQUENCES

The severity of the consequences of a security event at a facility is generally expressed in terms of the degree of injury or damage that would result if there were a successful attack. Malevolent acts may involve effects that are more severe than expected with accidental risk. Some examples of relevant consequences in a SVA include:

- Injuries to the public or to workers.
- Environmental damage.
- Direct and indirect financial losses to the company and to suppliers and associated businesses.
- Disruption to the national economy, regional, or local operations and economy.
- Loss of reputation or business viability.
- Need to evacuate people living or working near the facility.
- Excessive media exposure and related public concern affecting people that may be far removed from the actual event location.

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to cause maximize damage, so a worse credible security event should be defined. Critical infrastructure especially may have dependencies and interdependencies that need careful consideration.

In addition, theft of hazardous materials should be included in SVAs as applicable. Adversaries may be interested in theft of hazardous materials to either cause direct harm at a later date, use them for other illicit purposes such as illegal drug manufacturing, or possibly to make chemical weapons using the stolen materials as constituents.

Consequences are used as one of the key factors in determining the criticality of the asset and the degree of security countermeasures required. During the facility characterization step, consequences are used to screen low value assets from further consideration. For example, terrorists are assumed to be uninterested in low consequence assets (those that do not meet their criteria for valuable impacts).

2.4 ASSET ATTRACTIVENESS

Not all assets are of equal value to adversaries. A basic assumption of the SVA process is that this perception of value from an adversary's perspective is a factor that influences the likelihood of a security event. Asset attractiveness is an estimate of the real or perceived value of a target to an adversary based on such factors as shown in Figure 2.3.

During the SVA, the attractiveness of each asset should be evaluated based on the adversary's intentions or anticipated level of interest in the target. Security strategies can be developed around the estimated targets and potential threats. This factor, along with consequences, are used to screen facilities from more specific scenario analysis and from further specific countermeasures considerations during the first screening of the methodology.

Figure 2.3—Asset Attractiveness Factors

Type of effect:
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
Type of target:
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to a national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognition of the target

2.5 THREAT

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- Terrorists (international or domestic);
- Activists, pressure groups, single-issue zealots;
- Disgruntled employees or contractors;
- Criminals (e.g., white collar, cyber hacker, organized, opportunists).

Threat information is important reference data to allow the Owner/Operator to understand the adversaries interested in the assets of the facility, their operating history, their methods and capabilities, their possible plans, and why they are motivated. This information should then be used to develop a design basis threat or threats.

Adversaries may be categorized as occurring from three general types:

- Insider threats
- External threats
- Insiders working as colluders with external threats

Each applicable adversary type should be evaluated against each asset as appropriate to understand vulnerabilities.

2.6 VULNERABILITY

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. In a SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect, or analyzed by considering multiple potential specific sequences of events (a scenario-based approach). For this SVA methodology, each critical asset is analyzed from at least an asset-based approach at first by considering consequences and attractiveness. If it is a specific high value target, then it is recommended to analyze the asset further using scenarios.

2.7 SVA APPROACH

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of each facility from both the general viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the facility level, and outer perimeter analysis including access control and general physical security. For example, all facilities will maintain a minimum level of security with general countermeasures such as the plant access control strategy and administrative controls. Certain assets will justify a more specific level of security, such as additional surveillance or barriers, based on their value and expected level of interest to adversaries. The benefit of evaluating specific assets is that individual risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

This SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire facility, the assets that comprise the facility, the critical functions of the facility, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are ‘critical’ to the business operation. This is illustrated in Figure 2.4.

Criticality is defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance of the asset. For example, a storage tank of a hazardous material may not be the most critical part of the operation of a process, but if attacked, it has the greatest combined impact so it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary’s perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities.

As shown in Figure 2.4, all assets receive at least a general security review. This is accomplished by the SVA team's initial consideration of assets, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix B.

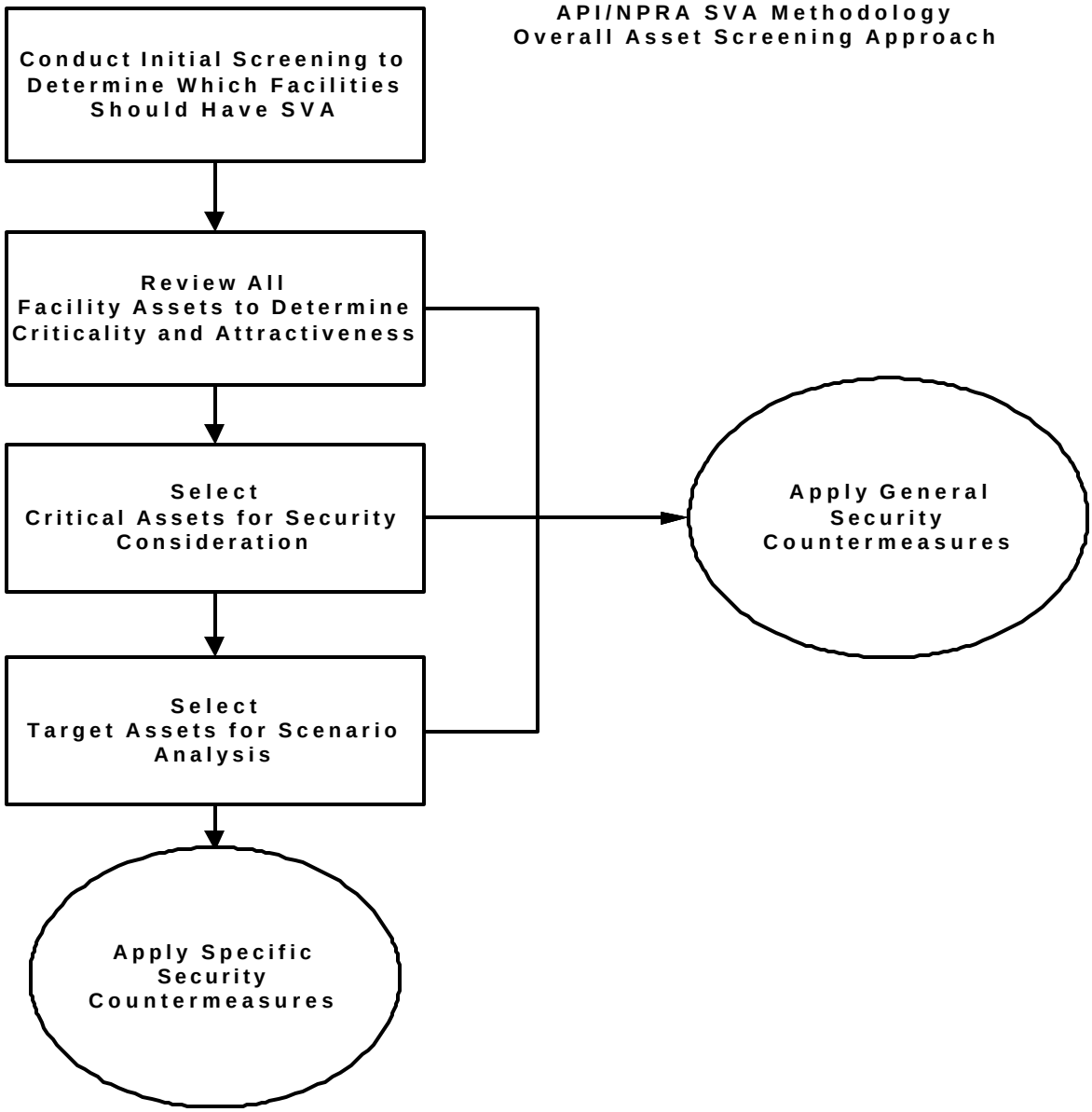


Figure 2.4—Overall Asset Screening Approach

All facilities should establish a security strategy. The general strategy is to protect against unauthorized access at the facility perimeter, and to control the access of authorized persons on the facility. Certain assets will be protected with added layers of protection, due to their attractiveness and consequences of loss. The specific security countermeasures provided to those assets would be to deter, detect, delay, and respond to credible threats against the assets to limit the risk to a certain level.

2.8 CHARACTERISTICS OF A SOUND SVA APPROACH

It is important to distinguish between a security risk management process and any given SVA methodology. Security risk management is the management framework that includes the SVA, development and implementation of a security plan, and the application of needed countermeasures to enhance security. SVA is the estimation of risk for the purposes of decision-making. SVA methodologies can be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks of a system. However, SVA methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. SVA methods should be used as part of a process that involves knowledgeable and experienced personnel that critically review the input, assumptions, and results. The SVA team should integrate the SVA output with other factors, the impact of key assumptions, and the impact of uncertainties created by the absence of data or the variability in assessment inputs before arriving at decisions about risk and actions to reduce risk.

A variety of different approaches to SVA have been employed in the petroleum sector as well as other industries. The major differences among approaches are associated with:

- The relative "mix" of knowledge, data, or logic SVA methods;
- The complexity and detail of the SVA method; and
- The nature of the output (probabilistic versus relative measures of risk).

Ultimately, it is the responsibility of the owner/operator to choose the SVA method that best meets the needs of the company, the facilities and the agencies tasked with providing additional security in times of imminent danger. Therefore, it is in the best interest of the owner/operator to develop a thorough understanding of the various SVA methods in use and available, as well as the respective strengths and limitations of the different types of methods, before selecting a long-term strategy. A SVA should be:

- **Risk-based—**The approach should be to focus on the most significant security issues in a priority order based on risk. Risk can also be used to judge the adequacy of existing security measures.
- **Structured—**The underlying methodology must be structured to provide a thorough assessment. Some methodologies employ a more rigid structure than others. More flexible structures may be easier to use; however, they generally require more input from subject matter experts. However, all SVA methods identify and use logic to determine how the data considered contributes to risk in terms of affecting the likelihood and/or consequences of potential incidents.
- **Given adequate resources—**Appropriate personnel, time, and financial resources must be allocated to fit the detail level of the assessment.
- **Experience-based—**The frequency and severity of past security related events and the potential for future events should be considered. It is important to understand and account for any actions that have been made to prevent security related events. The SVA should consider the system-specific data and other knowledge about the system that has been acquired by field, operations, and engineering personnel as well as external expertise.
- **Predictive—**A SVA should be investigative in nature, seeking to identify recognized as well as previously unrecognized threats to the facility service and integrity. It should make use of previous security related events, but focus on the potential for future events, including the likelihood of scenarios that may never have happened before.
- **Based on the use of appropriate data**—Some SVA decisions are judgment calls. However, relevant data and particularly data about the system under review should affect the confidence level placed in the decisions.
- **Able to provide for and identify means of feedback—**SVA is an iterative process. Actual field drills, audits, and data collection efforts from both internal and external sources should be used to validate (or invalidate) assumptions made.

2.9 SVA STRENGTHS AND LIMITATIONS

Each of the SVA methods commonly used has its strengths and limitations. Some approaches are well suited to particular applications and decisions, but may not be as helpful in other situations. In selecting or applying SVA methods, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

- Does the scope of the SVA method encompass and identify significant security related events and risks of the facility or along the system? If not, how can the risks that are not included in the SVA method be assessed and integrated in the future?
- Will all data be assessed, as it really exists along the system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, e.g. station-by-station or mile-by-mile, dependent on the evaluation needs?
- What is the logical structure of variables that are evaluated to provide the qualitative and quantitative results of the SVA? Does this provide for straightforward data assimilation and assessment?
- Does the SVA method use numerical weights and other empirical factors to derive the risk measures and priorities? Are these weights based on the experience of the system, operator, industry, or external sources?
- Do the basic input variables of the SVA method require data that are available to the operator? Do operator data systems and industry data updating procedures provide sufficient support to apply the SVA method effectively? What is the process for updating the SVA data to reflect changes in the system, the infrastructure, and new security related data? How is the input data validated to ensure that the most accurate, up-to-date depiction of the system is reflected in the SVA?
- Does the SVA output provide adequate support for the justification of risk-based decisions? Are the SVA results and output documented adequately to support justification of the decisions made using this output?
- Does the SVA method allow for analysis of the effects of uncertainties in the data, structure, and parameter values on the method output and decisions being supported? What sensitivity or uncertainty analysis is supported by the SVA method?
- Does the SVA method focus exclusively on RMP-based “worst case” events or is it structured to determine “most probable worst case” events that may at times be less severe than postulated in an RMP or include additive effects of adjacent assets to yield consequences more severe than postulated in the RMP?

2.10 RECOMMENDED TIMES FOR CONDUCTING AND REVIEWING THE SVA

The SVA process or SVA methods can be applied at different stages of the overall security assessment and evaluation process. For example, it can be applied to help select, prioritize, and schedule the locations for security assessments. It can also be performed after the security assessment is completed to conduct a more comprehensive SVA that incorporates more accurate information about the facility or pipeline segment.

There are six occasions when the SVA may be required, as illustrated in Figure 2.5.

2.11 VALIDATION AND PRIORITIZATION OF RISKS

Independent of the process used to perform a SVA, the owner/operator must perform a quality control review of the output to ensure that the methodology has produced results consistent with the objectives of the assessment. This can be achieved through a review of the SVA data and results by a knowledgeable and experienced individual or, preferably, by a cross-functional team consisting of a mixture of personnel with skill sets and experience-based knowledge of the systems or segments being reviewed. This validation of the SVA method should be performed to ensure that the method has produced results that make sense to the operator. If the results are not consistent with the operator’s understanding and expectations of system operation and risks, the operator should explore the reasons why and make appropriate adjustments to the method, assumptions, or data. Some additional criteria to evaluate the quality of a SVA are:

- Are the data and analyses handled competently and consistently throughout the system? (Can the logic be readily followed?)
- Is the assessment presented in an organized and useful manner?
- Are all assumptions identified and explained?
- Are major uncertainties identified, e.g., due to missing data?
- Do evidence, analysis, and argument adequately support conclusions and recommendations?

Once the SVA method and process has been validated, the operator has the necessary information to prioritize risks. To determine what risk mitigation actions to take, the operator considers which systems (or segments of systems) have the highest risks and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

2.12 RISK SCREENING

Security issues exist at every facility managed by the petroleum and petrochemical industry, but the threat of intentional acts is likely to be different across the industry. This is captured by the factor known as 'asset attractiveness', whereby certain assets are considered to be more attractive to adversaries than others. Based on many reported threat assessments, intelligence reports, and actual events around the world, these factors can be used to evaluate target attractiveness.

It is likely that most facilities have no specific threat history for terrorism. As a result, the assumption must be made that potential malevolent acts are generally credible at each facility and this is then tempered by the site-specific factors. A screening process may contain the following factors:

1. Target attractiveness or target value;
2. Degree of threat;
3. Vulnerability;
4. Potential consequences (casualties, environmental, infrastructure and economic).

These are the same factors as are used for evaluating an individual asset risk, but the difference is that this is done at a generalized facility level for the risk screening instead of at a target asset level. Note that target attractiveness itself includes the factors of consequences and vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting. Consequences are listed again separately since they have such importance in targeting.

Consequence and target attractiveness are the dominant factors in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk dilemma. Priority should first be given to the consequence ranking, but then consideration should be given to the attractiveness ranking when making assessments. In this way resources can be appropriately applied to assets where they are most likely to be important. This philosophy may be adopted by a company at an enterprise level to help determine both the need to conduct detailed (vs. simpler checklist analyses or audits), and the priority order for the analysis.

Figure 2.5—Recommended Times for Conducting and Reviewing the SVA

1	An initial review of all relevant facilities and assets per a schedule set during the initial planning process
2	When an existing process or operation is proposed to be substantially changed and prior to implementation (revision or rework)
3	When a new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the manager of the facility (revision or rework)
5	After a significant security incident, at the discretion of the manager of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

Chapter 3 Conducting the Security Vulnerability Assessment Methodology

3.1 OVERVIEW OF THE SVA METHODOLOGY

The SVA process is a risk-based and performance-based methodology. The user can choose different means of accomplishing the general SVA method so long as the end result meets the same performance criteria. The overall 5-step approach of the SVA methodology is described as follows:

Step 1: Asset Characterization

The asset characterization includes analyzing information that describes the technical details of facility assets as required to support the analysis, identifying the potential critical assets, identifying the hazards and consequences of concern for the facility and its surroundings and supporting infrastructure, and identifying existing layers of protection.

Step 2: Threat Assessment

The consideration of possible threats should include internal threats, external threats, and internally assisted threats (i.e., collusion between insiders and outside agents). The selection of the threats should include reasonable local, regional, or national intelligence information, where available. This step includes determining the target attractiveness of each asset from each adversary's perspective.

Step 3: Vulnerability Analysis

The vulnerability analysis includes the relative pairing of each target asset and threat to identify potential vulnerabilities related to process security events. This involves the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities.

The degree of vulnerability of each valued asset and threat pairing is evaluated by the formulation of security-related scenarios or by an asset protection basis. If certain criteria are met, such as higher consequence and attractiveness ranking values, then it may be useful to apply a scenario-based approach to conduct the Vulnerability Analysis. It includes the assignment of risk rankings to the security-related scenarios developed. If the asset-based approach is used, the determination of the asset's consequences and attractiveness may be enough to assign a target ranking value and protect via a standard protection set for that target level. In this case, scenarios may not be developed further than the general thought that an adversary is interested in damaging or stealing an asset.

Step 4: Risk Assessment

The risk assessment determines the relative degree of risk to the facility in terms of the expected effect on each critical asset as a function of consequence and probability of occurrence. Using the assets identified during Step 1 (Asset Characterization), the risks are prioritized based on the likelihood of a successful attack. Likelihood is determined by the team after considering the attractiveness of the targeted assets assessed under Step 2, the degree of threats assessed under Step 2, and the degree of vulnerability identified under Step 3.

Step 5: Countermeasures Analysis

Based on the vulnerabilities identified and the risk that the layers of security are breached, appropriate enhancements to the security countermeasures may be recommended. Countermeasure options will be identified to further reduce vulnerability at the facility. These include improved countermeasures that follow the process security doctrines of deter, detect, delay, respond, mitigate and possibly prevent. Some of the factors to be considered are:

- Reduced probability of successful attack
- Degree of risk reduction by the options
- Reliability and maintainability of the options
- Capabilities and effectiveness of mitigation options
- Costs of mitigation options
- Feasibility of the options

The countermeasure options should be re-ranked to evaluate effectiveness, and prioritized to assist management decision making for implementing security program enhancements. The recommendations should be included in a SVA report that can be used to communicate the results of the SVA to management for appropriate action.

Once the SVA is completed, there is a need to follow-up on the recommended enhancements to the security countermeasures so they are properly reviewed, tracked, and managed until they are resolved. Resolution may include adoption of the SVA team's recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Rejection of a SVA recommendation and related acceptance of residual risk should be based on valid reasons that are well documented.

This SVA process is summarized in Figure 3.1 and illustrated further in the flowcharts that follow in Figures 3.1a through 3.1c. Section 3.2 of this chapter describes the preparation activities, such as data gathering and forming the SVA team. Sections 3.3 through 3.8 provide details for each step in the SVA methodology. These steps and associated tasks are also summarized in Figure 3.5.

Figure 3.1—Security Vulnerability Assessment Methodology Steps

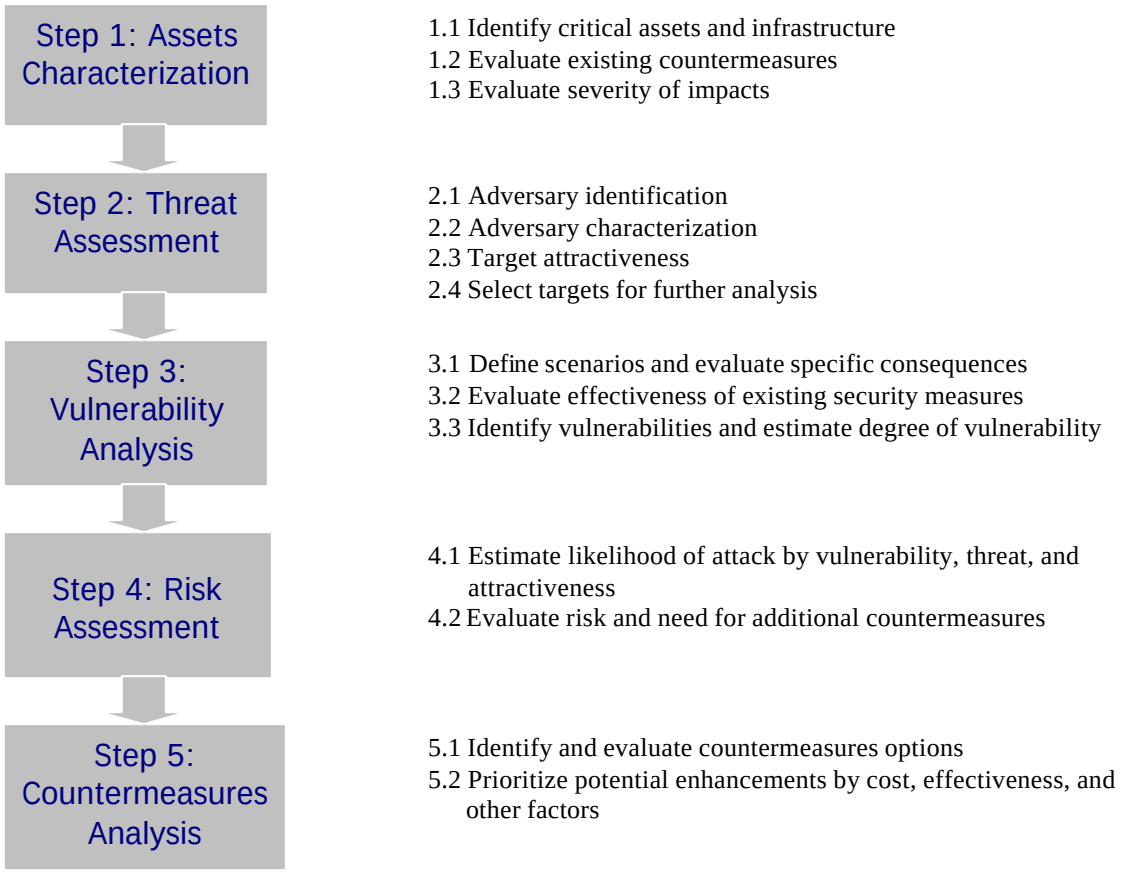


Figure 3.1a—Security Vulnerability Assessment Methodology—Step 1

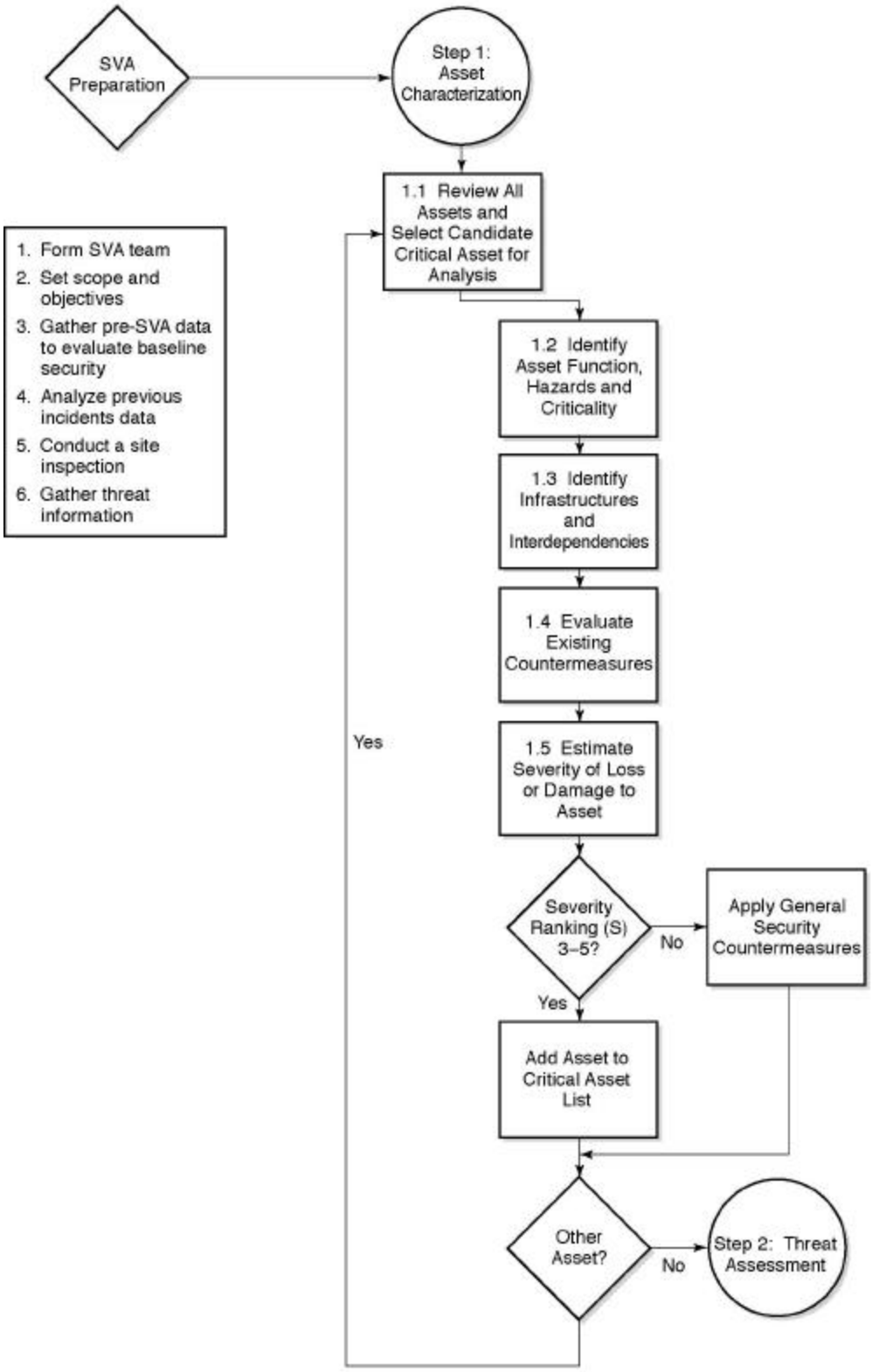


Figure 3.1b—Security Vulnerability Assessment Methodology—Step 2

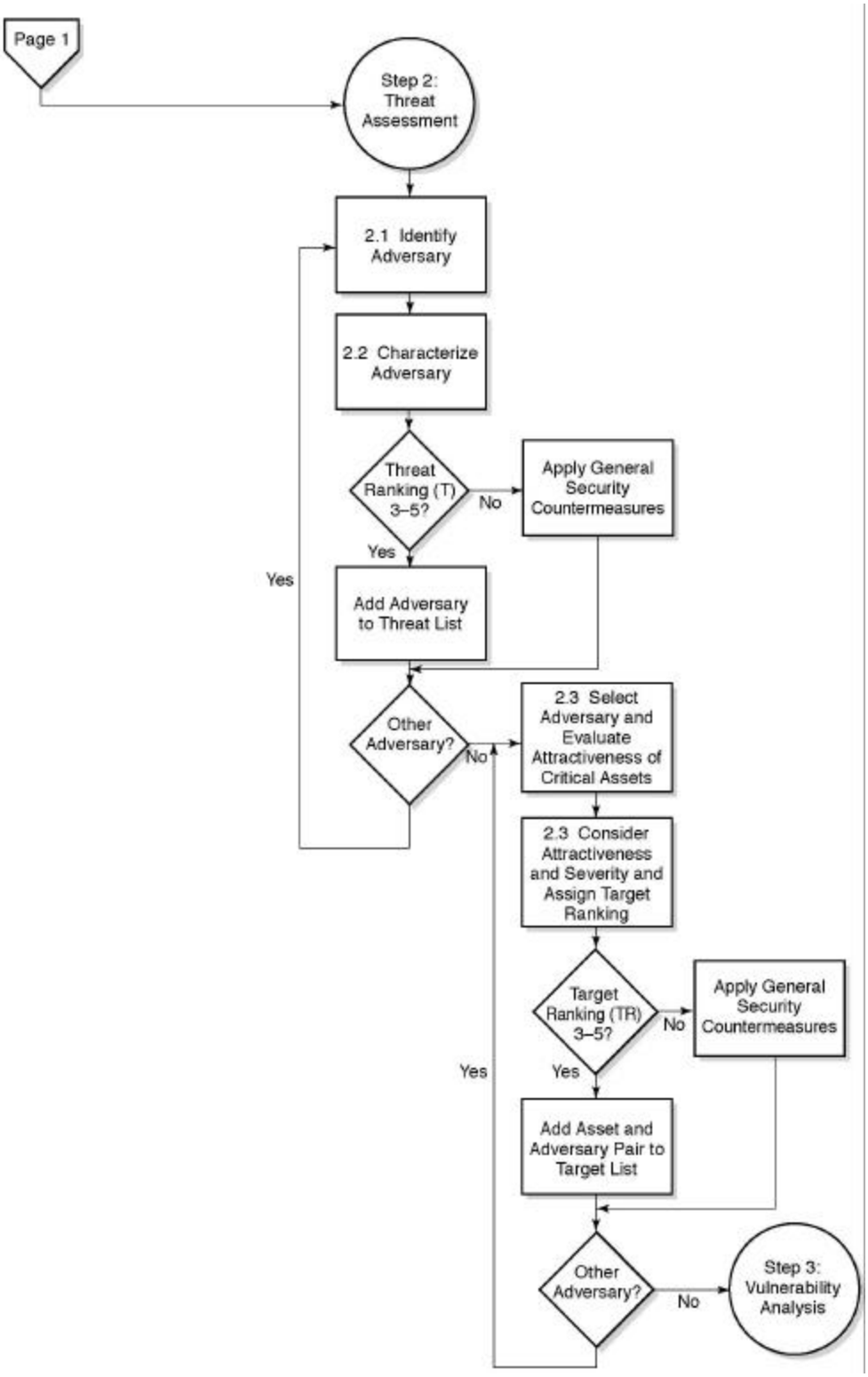
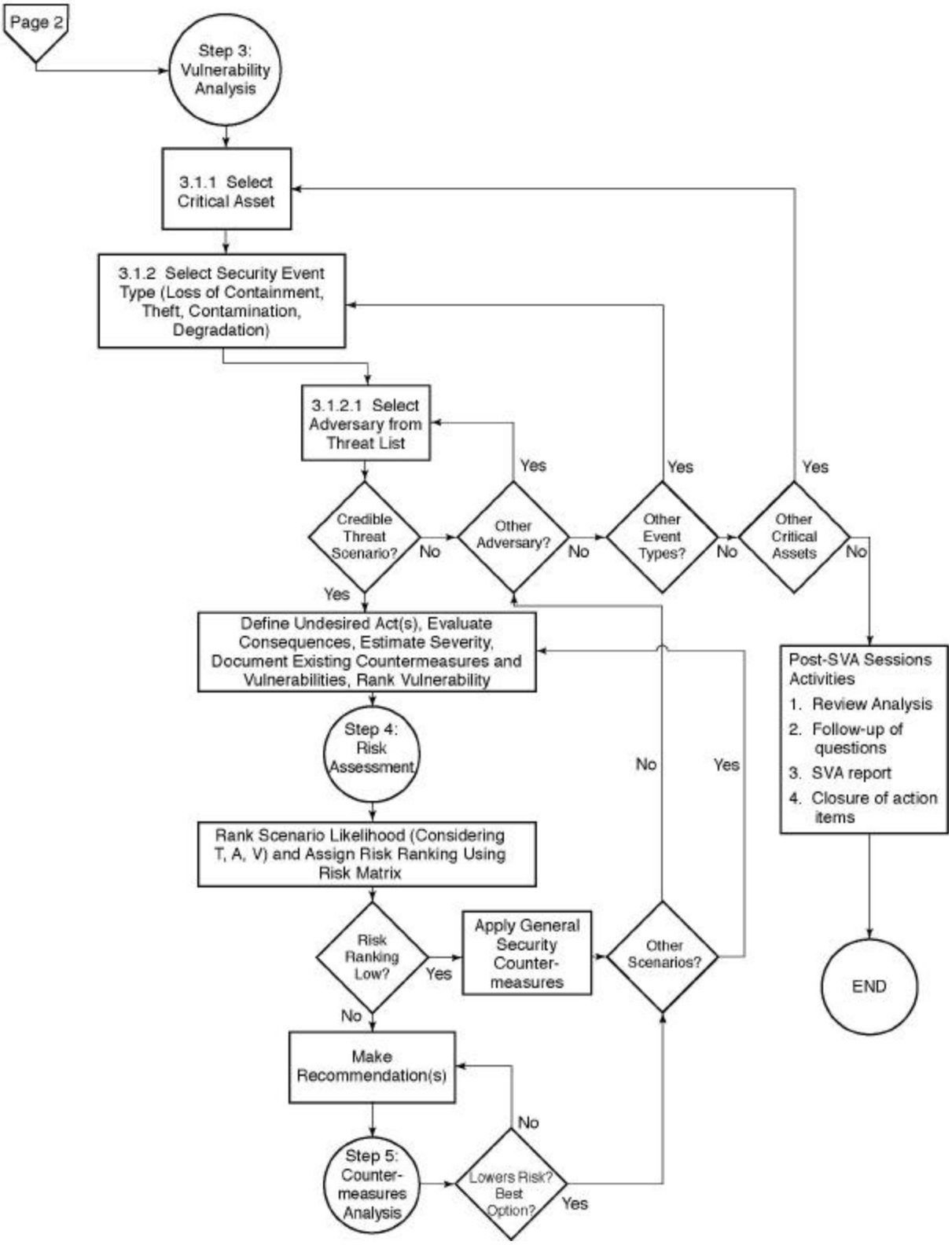


Figure 3.1c—Security Vulnerability Assessment Methodology—Steps 3 – 5



3.2 SVA PREPARATION

3.2.1 Planning for Conducting a SVA

Prior to conducting the SVA team-based sessions, there are a number of activities that must be done to ensure an efficient and accurate analysis. There are many factors in successfully completing a SVA including the following:

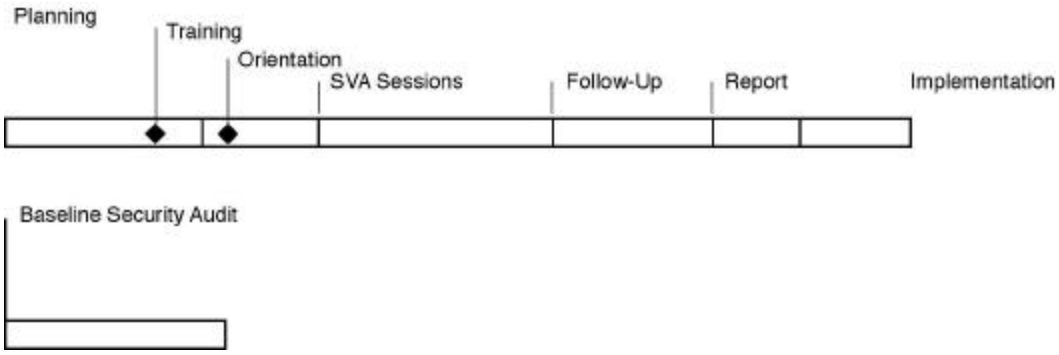
- the activity should be planned well in advance;
- have the full support and authorization by management to proceed;
- the data should be verified and complete;
- the objectives and scope should be concise;
- the team should be knowledgeable of and experienced at the process they are reviewing; and,
- the team leader should be knowledgeable and experienced in the SVA process methodology.

All of the above items are controllable during the planning stage prior to conducting the SVA sessions. Most important for these activities is the determination of SVA specific objectives and scope, and the selection and preparation of the SVA Team.

Prerequisites to conducting the SVA include gathering study data, gathering and analyzing threat information, forming a team, training the team on the method to be used, conducting a baseline security survey, and planning the means of documenting the process.

The typical timeline for conducting a SVA is shown in Figure 3.2.

Figure 3.2—SVA Methodology Timeline



3.2.2 SVA Team

The SVA approach includes the use of a representative group of company experts plus outside experts if needed to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the operator's system. These experts draw on the years of experience, practical knowledge, and observations from knowledgeable field operations and maintenance personnel in understanding where the security risks may reside and what can be done to mitigate or ameliorate them.

Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts should focus on the vulnerabilities that would enhance the effectiveness of the facility security plan. The primary goal of this group is to capture and build into the SVA method the experience of this diverse group of individual experts so that the SVA process will capture and incorporate information that may not be available in typical operator databases.

If the scope of the SVA includes terrorism and attacks on a process handling flammable or toxic substances, the SVA should be conducted by a team with skills in both the security and process safety areas. This is because the team must evaluate traditional facility security as well as process–safety related vulnerabilities and countermeasures. The final security strategy for protection of the process assets from these events is a combination of security and process safety strategies.

It is expected that a full time 'core' team is primarily responsible, and that they are led by a Team Leader. Other part-time team members, interviewees and guests are used as required for efficiency and completeness. At a minimum, SVA

teams should possess the knowledge and/or skills listed in Figure 3.3. Other skills that should be considered and included, as appropriate, are included as optional or part-time team membership or as guests and persons interviewed.

The SVA Core Team is typically made up of three to five persons, but this is dependent on the number and type of issues to be evaluated and the expertise required to make those judgments. The Team Leader should be knowledgeable and experienced in the SVA approach.

3.2.3 SVA Objectives and Scope

The SVA Team leader should develop an objectives and scope statement for the SVA. This helps to focus the SVA and ensure completeness. An example SVA objectives statement is shown in Figure 3.4.

A work plan should then be developed to conduct the SVA with a goal of achieving the objectives. The work plan needs to include the scope of the effort, which includes which physical or cyber facilities and issues will be addressed.

Given the current focus on the need to evaluate terrorist threats, the key concerns are the intentional (malevolent) misuse of petroleum and hazardous to cause catastrophic consequences. Given this focus, the key events and consequences of interest include the four listed in Figure 3.5. Other events may be included in the scope as determined by the SVA Team, but it is recommended that these four primary security events be addressed first since these are the events that make the petroleum and petrochemical industry unique from other industries.

Figure 3.3—SVA Team Members

The SVA Core Team members should have the following skill sets and experience:

- Team leader—knowledge of and experience with the SVA methodology;
- Security representative—knowledge of facility security procedures, methods and systems;
- Safety representative—knowledge of potential process hazards, process safety procedures, methods, and systems of the facility;
- Facility representative—knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures;
- Operations representative—knowledge of the facility process and equipment operation;
- Information systems/Automation representative (for cyber security assessment) —knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.

The SVA Optional/Part-time Team members may include the following skill sets and experience:

- Security specialist—knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available;
- Cyber security specialist—knowledge of cyber security practices and technologies;
- Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.;
- Process specialist—knowledge of the process design and operations
- Management—knowledge of business management practices, goals, budgets, plans, and other management systems.

Figure 3.4—Sample Objectives Statement[8]

To conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company.

[7]Ibid, AIChE.
[8]Ibid, AIChE.

Figure 3.5—Security Events of Concern

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	Loss of containment of process hydrocarbons or hazardous chemicals on the plant site from intentional damage of equipment or the malicious release of process materials, which may cause multiple casualties, severe damage, and public or environmental impact. Also included is injury to personnel and the public directly or indirectly
Theft	Hydrocarbon, chemical, or information theft or misuse with the intent to cause severe harm at the facility or offsite
Contamination	Contamination or spoilage of plant products or information to cause worker or public harm on or offsite
Degradation of Assets	Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive acts of terrorism.

3.2.4 Data Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for Owner/Operators to obtain the data needed to manage the security of their facility. Most Owner/Operators will find that many of the data elements suggested here are already being collected. This section provides a systematic review of potentially useful data to support a security plan. However, it should be recognized that all of the data elements in this section are not necessarily applicable to all systems.

The types of data required depend on the types of risks and undesired acts that are anticipated. The operator should consider not only the risks and acts currently suspected in the system, but also consider whether the potential exists for other risks and acts not previously experienced in the system, e.g., bomb blast damage. This section includes lists of many types of data elements. The following discussion is separated into four subsections that address sources of data, identification of data, location of data, and data collection and review.

Appendix A includes a list of potentially useful data that may be needed to conduct a SVA. Appendix B is a checklist of countermeasures that may be used as a data collection form prior to conducting a SVA. Similarly, Appendix C is a checklist for infrastructure and interdependencies that can be used both before and after a SVA for ensuring completeness.

3.2.4.1 Data Sources

The first step in gathering data is to identify the sources of data needed for facility security management. These sources can be divided into four different classes.

1. **Facility and Right of Way Records.** Facility and right of way records or experienced personnel are used to identify the location of the facilities. This information is essential for determining areas and other facilities that either may impact or be impacted by the facility being analyzed and for developing the plans for protecting the facility from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various potentially exposed areas surrounding the facility i.e., population centers, and industrial and government facilities.
2. **System Information.** This information identifies the specific function of the various parts of the process and their importance from a perspective of identifying the security risks and mitigations as well as understanding the alternatives to maintaining the ability of the system to continue operations when a security threat is identified. This information is also important from a perspective of determining those assets and resources available in-house in developing and completing a security plan. Information is also needed on those systems in place, which could support a security plan such as an integrity management program and IT security functions.
3. **Operation Records.** Operating data are used to identify the products transported and the operations as they may pertain to security issues to facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, e.g., type of product, facility type and location, and volumes transported. Included in operation records data gathering is the need to obtain incident data to capture historical security events.
4. **Outside Support and Regulatory Issues.** This information is needed for each facility or pipeline segment to determine the level of outside support that may be needed and can be expected for the security measures to be employed at each facility or pipeline segment. Data are also needed to understand the expectation for security preparedness and coordination from the regulatory bodies at the government, state, and local levels. Data should also be developed on communication and other infrastructure issues as well as sources of information regarding security threats, e.g., ISACs (Information Sharing and Analysis Centers).

3.2.4.2 Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the SVA methodology selected, and the decisions that are to be made. The data collection approach will follow the SVA path determined by the initial expert team assembled to identify the data needed for the first pass at SVA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the SVA team to begin their work with an overview or screening assessment of the most critical issues that impact the facility or pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this SVA. As the SVA process evolves, the scope of the data collection will be expanded to support more detailed assessment of perceived areas of vulnerability.

3.2.4.3 Locating Required Data

Operator data and information are available in different forms and format. They may not all be physically stored and updated at one location based on the current use or need for the information. The first step is to make a list of all data required for security vulnerability assessment and locate the data. The data and information sources may include:

- Facility plot plans, equipment layouts and area maps
- Process and Instrument Drawings (P&IDs)
- Pipeline alignment drawings
- Existing company standards and security best practices
- Product throughput and product parameters
- Emergency response procedures
- Company personnel interviews
- LEPC (Local Emergency Planning Commission) response plans
- Police agency response plans
- Historical security incident reviews
- Support infrastructure reviews

3.2.4.4 Data Collection and Review

Every effort should be made to collect good quality data. When data of suspect quality or consistency are encountered, such data should be flagged so that during the assessment process, appropriate confidence interval weightings can be developed to account for these concerns.

In the event that the SVA approach needs input data that are not readily available, the operator should flag the absence of information. The SVA team can then discuss the necessity and urgency of collecting the missing information

3.2.5 Analyzing Previous Incidents Data

Any previous security incidents relevant to the security vulnerability assessment may provide valuable insights to potential vulnerabilities and trends. These events from the site and, as available, from other historical records and references, should be considered in the analysis. This may include crime statistics, case histories, or intelligence relevant to facility.

3.2.6 Conducting a Site Inspection

Prior to conducting the SVA sessions, it is necessary for the team to conduct a site inspection to visualize the facility and to gain valuable insights to the layout, lighting, neighboring area conditions, and other facts that may help understand the facility and identify vulnerabilities. The list of data requirements in Appendix A and the checklist in Appendix B may be referenced for this purpose.

3.2.7 Gathering Threat Information

The team should gather and analyze relevant company and industry or government-provided threat information, such as that available from the Energy ISAC, DHS, FBI, or other local law enforcement agency.

3.3 STEP 1: ASSETS CHARACTERIZATION

Characterization of the facility is a step whereby the facility assets and hazards are identified, and the potential consequences of damage or theft to those assets is analyzed. The focus is on processes which may contain petroleum or hazardous chemicals and key assets, with an emphasis on possible public impacts. The Asset Attractiveness, based on

these and other factors, is included in the facility characterization. These two factors (severity of the consequences and asset attractiveness) are used to screen the facility assets into those that require only general vs. those that require more specific security countermeasures.

The team produces a list of candidate critical assets that need to be considered in the analysis. Attachment 1—Step 1: Critical Assets/Criticality Form is helpful in developing and documenting the list of critical assets. The assets may be processes, operations, personnel, or any other asset as described in Chapter 3.

Figure 3.6 below summarizes the key steps and tasks required for Step 1.

Step 1.1—Identify Critical Assets

The SVA Team should identify critical assets for the site being studied. The focus is on petroleum or chemical process assets, but any asset may be considered. For example, the process control system may be designated as critical, since protection of it from physical and cyber attack may be important to prevent a catastrophic release or other security event of concern. Figure 3.7 is an example list of specific assets that may be designated as critical at any given site. Assets include the full range of both material and non-material aspects that enable a facility to operate.

Figure 3.6—Description of Step 1 and Substeps

Step	Task
Step 1: Assets Characterization	
1.1 Identify critical assets	Identify critical assets of the facility including people, equipment, systems, chemicals, products, and information.
1.2 Identify critical functions	Identify the critical functions of the facility and determine which assets perform or support the critical functions.
1.3 Identify critical infrastructures and interdependencies	Identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset.
1.4 Evaluate existing countermeasures	Identify what protects and supports the critical functions and assets. Identify the relevant layers of existing security systems including physical, cyber, operational, administrative, and business continuity planning, and the process safety systems that protect each asset.
1.5 Evaluate impacts	Evaluate the hazards and consequences or impacts to the assets and the critical functions of the facility from the disruption, damage, or loss of each of the critical assets or functions.
1.6 Select targets for further analysis	Develop a target list of critical functions and assets for further study.

Figure 3.7—Example Candidate Critical Assets

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	• Process equipment handling petroleum and hazardous materials including processes, pipelines, storage tanks • Marine vessels and facilities, pipelines, other transportation systems • Employees, contractors, visitors in high concentrations
Theft	• Hydrocarbons or chemicals processed, stored, manufactured, or transported • Metering stations, process control and inventory management systems • Critical business information from telecommunications and information management systems including Internet accessible assets
Contamination	• Raw material, intermediates, catalysts, products, in processes, storage tanks, pipelines • Critical business or process data
Degradation of Assets	• Processes containing petroleum or hazardous chemicals • Business image and community reputation • Utilities (electric power, steam, water, natural gas, specialty gases) • Telecommunications Systems • Business systems

The following information should be reviewed by the SVA Team as appropriate for determination of applicability as critical assets:

- Any applicable regulatory lists of highly hazardous chemicals, such as the Clean Air Act 112(r) list of flammable and toxic substances for the EPA Risk Management Program (RMP) 40 *CFR* Part 68 or the OSHA Process Safety Management (PSM) 29 *CFR* 1910.119 list of highly hazardous chemicals;
- Inhalation poisons or other chemicals that may be of interest to adversaries;
- Large and small scale chemical weapons precursors as based on the following lists:
  - Chemical Weapons Convention list;
  - FBI Community Outreach Program (FBI List) for Weapons of Mass Destruction materials and precursors;
  - The Australia Group list of chemical and biological weapons
- Material destined for the food, nutrition, cosmetic or pharmaceutical chains;
- Chemicals which are susceptible to reactive chemistry.

Owner/Operators may wish to consider other categories of chemicals that may cause losses or injuries that meet the objectives and scope of the analysis. These may include other flammables, critically important substances to the process, explosives, radioactive materials, or other chemicals of concern.

In addition, the following personnel, equipment and information may be determined to be critical:

- Process equipment
- Critical data
- Process control systems
- Personnel
- Critical infrastructure and support utilities

Step 1.2—Identify Critical Functions

The SVA Team should identify the critical functions of the facility and determine which assets perform or support the critical functions. For example, the steam power plant of a refinery may be critical since it is the sole source of steam supply to the refinery.

Step 1.3—Identify Critical Infrastructures and Interdependencies

The SVA team should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline. Appendix C, Interdependencies and Infrastructure Checklist, can be used to identify and analyze these issues. Note that some of these issues may be beyond the control of the owner/operator, but it is necessary to understand the dependencies and interdependencies of the facility, and the result of loss of these systems on the process.

Step 1.4—Evaluate Existing Countermeasures

The SVA team identifies and documents the existing security and process safety layers of protection. This may include physical security, cyber security, administrative controls, and other safeguards. During this step the objective is to gather information on the types of strategies used, their design basis, and their completeness and general effectiveness. A pre-SVA survey is helpful to gather this information. The data will be made available to the SVA team for them to form their opinions on the adequacy of the existing security safeguards during Step 3: Vulnerability Analysis and Step 5: Countermeasures Analysis.

Appendix B—Countermeasures Survey Form can be used to gather information on the presence and status of existing safeguards or another form may be more suitable. Existing records and documentation on security and process safety systems, as well as on the critical assets themselves, can be referenced rather than repeated in another form of documentation.

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. Appendix B contains checklists that may be used to conduct the physical security portion of the survey.
Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

Step 1.5—Evaluate Impacts

The Impacts Analysis step includes both the determination of the hazards of the asset being compromised as well as the specific consequences of a loss. The SVA team should consider relevant chemical use and hazard information, as well as information about the facility. The intent is to develop a list of target assets that require further analysis partly based on the degree of hazard and consequences. Particular consideration should be given to the hazards of fire, explosion, toxic release, radioactive exposure, and environmental contamination.

The consequences are analyzed to understand their possible significance. The Appendix A—Attachment 1—Step 1: Critical Assets/Criticality Form is useful to document the general consequences for each asset. The consequences may be generally described but consideration should be given to those listed in Figure 3.8.

Figure 3.8—Possible Consequences of Security Events

Public fatalities or injuries
Site personnel fatalities or injuries
Large-scale disruption to the national economy, public or private operations
Large-scale disruption to company operations
Large-scale environmental damage
Large-scale financial loss
Loss of critical data
Loss of reputation or business viability

The consequence analysis is done in a general manner. If the security event involves a toxic or flammable release to the atmosphere, the EPA RMP offsite consequence analysis guidance can be used as a starting point. If it is credible to involve more than the largest single vessel containing the hazardous material in a single incident, the security event may be larger than the typical EPA RMP worst-case analysis.

A risk ranking scale can be used to rank the degree of severity. Figure 3.9 illustrates a set of consequence definitions based on four categories of events—A. Fatalities and injuries; B. Environmental impacts; C. Property damage; and D. Business interruption.

Figure 3.9—Example Definitions of Consequences of the Event

DESCRIPTION	RANKING
A. Possible for any offsite fatalities from large-scale toxic or flammable release; possible for multiple onsite fatalities B. Major environmental impact onsite and/or offsite (e.g., large-scale toxic contamination of public waterway) C. Over $*X* property damage D. Very long term (> *X* years) business interruption/expense; Large-scale disruption to the national economy, public or private operations; Loss of critical data; Loss of reputation or business viability	**S5 – Very High**
A. Possible for onsite fatalities; possible offsite injuries B. Very large environmental impact onsite and/or large offsite impact C. Over $ *X* – $ *Y* property damage D. Long term (*X* months – *Y* years) business interruption/expense	**S4 – High**
A. No fatalities or injuries anticipated offsite; possible widespread onsite serious injuries B. Environmental impact onsite and/or minor offsite impact C. Over $ *X* -$ *Y* property damage D. Medium term (*X* months – *Y* months) business interruption/expense	**S3 – Medium**
A. Onsite injuries that are not widespread but only in the vicinity of the incident location; No fatalities or injuries anticipated offsite B. Minor environmental impacts to immediate incident site area only C. $ *X* – $ *Y* loss property damage D. Short term (up to *X* months) business interruption/expense	**S2 – Low**
A. Possible minor injury onsite; No fatalities or injuries anticipated offsite B. No environmental impacts C. Up to $*X* Property Damage D. Very short term (up to *X* weeks) business interruption/expense	**S1 – Very Low**

The consequences of a security event at a facility are generally expressed in terms of the degree of acute health effects (e.g., fatality, injury), property damage, environmental effects, etc. This definition of consequences is the same as that used for accidental releases, and is appropriate for security-related events. The key difference is that they may involve effects that are more severe than expected with accidental risk. This difference has been considered in the steps of the SVA.

The SVA Team should evaluate the potential consequences of an attack using the judgment of the SVA team. If scenarios are done, the specific consequences may be described in scenario worksheets.

Team members skilled and knowledgeable in the process technology should review any off-site consequence analysis data previously developed for safety analysis purposes or prepared for adversarial attack analysis. The consequence analysis data may include a wide range of release scenarios if appropriate.

Proximity to off-site population is a key factor since it is both a major influence on the person(s) selecting a target, and on the person(s) seeking to defend that target. In terms of attractiveness to a terrorist, if the target could expose a large number of persons, this type of target is likely to be a high-value, high-payoff target.

Step 1.6—Select Targets for Further Analysis

For each asset identified, the criticality of each asset must be understood. This is a function of the value of the asset, the hazards of the asset, and the consequences if the asset was damaged, stolen, or misused. For hazardous chemicals, consideration may include toxic exposure to workers or the community, or potential for the misuse of the chemical to produce a weapon or the physical properties of the chemical to contaminate a public resource.

The SVA Team develops a Target Asset List which is a list of the assets associated with the site being studied that are more likely to be attractive targets, based on the complete list of assets and the identified consequences and targeting issues identified in the previous steps. During Step 3: Vulnerability Analysis, the Target Asset List will be generally paired with specific threats and evaluated against the potential types of attack that could occur.

The SVA methodology uses ranking systems that are based on a scale of 1 –s 5 where 1 is the lowest value and 5 is the highest value. Based on the consequence ranking and criticality of the asset, the asset is tentatively designated a candidate critical target asset. The attractiveness of the asset will later be used for further screening of important assets.

3.4 STEP 2: THREAT ASSESSMENT

The threat assessment step involves the substeps shown in Figure 3.10.

Step 2.1—Adversary Identification

The next step is to identify specific classes of adversaries that may perpetrate the security-related events. The adversary characterization sub-step involves developing as complete an understanding as is possible of the adversary's history, capabilities and intent. A threat matrix is developed to generally pair the assets with each adversary class as shown in Attachment 1—Step 2: Threat Assessment Form.

Figure 3.10—Description of Step 2 and Substeps

Step	Task
Step 2: Threat Assessment	
2.1 Adversary identification	Evaluate threat information and identify threat categories and potential adversaries. Identify general threat categories. Consider threats posed by insiders, external agents (outsiders), and collusion between insiders and outsiders.
2.2 Adversary characterization	Evaluate each adversary and provide an overall threat assessment/ ranking for each adversary using known or available information. Consider such factors as the general nature/history of threat; specific threat experience/history to the facility/operation; known capabilities/methods/weapons; potential actions, intent/ motivation of adversary.
2.3 Analyze target attractiveness	Conduct an evaluation of target (from assets identified in Step 1) attractiveness from the adversary perspective.

Depending on the threat, the analyst can determine the types of potential attacks and, if specific information is available (intelligence) on potential targets and the likelihood of an attack, specific countermeasures may be taken. Information may be too vague to be useful, but SVA Teams should seek available information from Federal, State, and Local law enforcement officials in analyzing threats. Absent specific threat information, the SVA can still be applied based on assuming general capabilities and characteristics of typical hypothetical adversaries.

Threat assessment is an important part of a security management system, especially in light of the emergence of international terrorism in the United States. There is a need for understanding the threats facing the industry and any given facility or operation to properly respond to those threats. This section describes a threat assessment approach as part of the security management process. Later in Section 3.0 the use of the threat assessment in the SVA process will be more fully explained.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of an attack.

Threat assessment is a process that must be systematically done and kept current to be useful. The determination of these threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of required countermeasures to manage the threats. Without a design basis threat or situation specific threat in mind, a company cannot effectively develop a cost-effective security management system.

In characterizing the threat to a facility or a particular asset for a facility, a company should examine the historical record of security events and obtains available general and location-specific threat information from government organizations and other sources. It should then evaluate these threats in terms of company assets that represent likely targets.

Some threats are assumed continuous, whereas others are assumed to be variable. As such, this guidance follows the Department of Homeland Security's Homeland Security Advisory System (HSAS) and the U.S.C.G. Maritime Security (MARSEC) security levels for management of varying threat levels to the industry. The threat assessment determines the estimated general threat level, which varies as situations develop. Depending on the threat level, different security measures over baseline measures will likely be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated often, threat assessments might not adequately capture emerging threats posed by some adversary groups. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Consequently, a threat assessment must be accompanied by a vulnerability assessment to provide better assurance of preparedness for a terrorist or other adversary attack.

Intelligence and law enforcement agencies assess the foreign and domestic terrorist threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The FBI gathers information and assesses the threat posed by domestic sources of terrorism.

Threat information gathered by both the intelligence and law enforcement communities can be used to develop a company-specific threat assessment. A company attempts to identify threats in order to decide how to manage risk in a cost-effective manner. All companies are exposed to a multitude of threats, including terrorism or other forms of threat.

A threat assessment can take different forms, but the key components are:

1. Identification of known and potential adversaries;
2. Recognition and analysis of their intentions, motivation, operating history, methods, weapons, strengths, weaknesses, and intelligence capabilities;
3. Assessment of the threat posed by the adversary factors mentioned above against each asset, and the assignment of an overall criticality ranking for each adversary.

Threats need to be considered from both insiders and outsiders, or a combination of those adversaries working in collusion. Insiders are defined as those individuals who normally have authorized access to the asset. They pose a particularly difficult threat, due to the possibility for deceit, deception, training, knowledge of the facilities, and unsupervised access to critical information and assets.

The threat categories to be considered are those that include intent and capability of causing major catastrophic harm to the facilities and to the public or environment. Typical adversaries that may be included in a SVA are: international terrorists, domestic terrorists (including disgruntled individuals/'lone wolf' sympathizers), disgruntled employees, or extreme activists.

All companies are encouraged to discuss threats with local and Federal law enforcement officials, and to maintain networking with fellow industrial groups to improve the quality of applicable threat information.

The threat assessment is not necessarily based on perfect information. In fact, for most facilities, the best available information is vague or nonspecific to the facility. A particularly frustrating part of the analysis can be the absence of site-specific information on threats. A suggested approach is to make an assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat. Site-specific information adjusts the generic average rankings accordingly.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats facing the assets. At that time the company's threat assessment should be referred to and possibly updated as required given additional information and analysis of vulnerabilities.

Figure 3.11 includes a five level ranking system for defining threats against an asset.

Step 2.2—Adversary Characterization

Insiders, outsiders or a combination of the two may perpetrate an attack. Insiders are personnel that have routine, unescorted access within the facility. Outsiders do not. Collusion between the two may be the result of monetary gain (criminal insider/terrorist outsider), ideological sympathy, or coercion.

The adversary characterization will assist in evaluating the attack issues associated with insider, outsider, and colluding adversary threats. The SVA team should consider each type of adversary identified as credible, and generally define their level of capabilities, motivation, and likelihood of threat.

Step 2.3—Analyze Target Attractiveness

The team assigns the target attractiveness ranking. To facilitate this use Attachment 1—Threat Assessment: Target Attractiveness Form can be used.

The attractiveness of the target to the adversary is a key factor in determining the likelihood of an attack. Examples of issues that may be addressed here include:

- Proximity to a symbolic or iconic target, such as a national landmark
- Unusually high corporate profile among possible terrorists, such as a major defense contractor
- Any other variable not addressed elsewhere, when the SVA Team agrees it has an impact on the site's value as a target or on the potential consequences of an attack.

The SVA Team should use the best judgment of its subject matter experts to assess attractiveness. This is a subjective process as are all vulnerability assessments whether qualitative or quantitative in nature.

Each asset is analyzed to determine the factors that might make it a more or less attractive target to the adversary. Attractiveness is used to assess likelihood of the asset being involved in an incident.

Target Attractiveness is an assessment of the target's value from the adversary's perspective, which is one factor used as a surrogate measure for likelihood of attack. Note that target attractiveness itself includes the other factors of consequences and difficulty of attack/vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting and anti-terrorism efforts. Arguably target attractiveness is the dominant factor in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk assessment dilemma.

The attractiveness of assets varies with the adversary threat including their motivation, intent, and capabilities. For example, the threat posed by an international terrorist and the assets they might be interested in could greatly vary from the threat and assets of interest to a violent activist or environmental extremist.

Figure 3.12 shows the factors that should be evaluated when evaluating target attractiveness for terrorism. The team can use these factors and rank each asset against each adversary by the scale shown in Figure 3.13. Other adversaries may be interested in other factors, and the user of the SVA is encouraged to understand the relevant factors and substitute them for those in Figure 3.12 as applicable.

3.5 SVA STEP 3: VULNERABILITY ANALYSIS

The Vulnerability Analysis step involves three steps, as shown in Figure 3.14. Once the SVA Team has determined how an event can be induced, it should determine how an adversary could make it occur. There are two schools of thought on methodology: the scenario-based approach and the asset-based approach. Both approaches are identical in the beginning, but differ in the degree of detailed analysis of threat scenarios and specific countermeasures applied to a given scenario. The assets are identified, and the consequences and target attractiveness are analyzed as per Step 2, for both approaches. Both approaches result in a set of annotated potential targets, and both approaches may be equally successful at evaluating security vulnerabilities and determining required protection.

Figure 3.11—Threat Rating Criteria

Threat Level	Description
5 – Very High	Indicates that a credible threat exists against the asset and that the adversary demonstrates the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis.
4 – High	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset or similar assets.
3 – Medium	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise similar assets.
2 – Low	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the assets.
1 – Very Low	Indicates no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets.

Figure 3.12—Target Attractiveness Factors (for Terrorism)

Type of effect:
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
Type of target:
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognition of the target

Figure 3.13—Attractiveness Factors Ranking Definitions (A)

Ranking Levels	Adversary Ranking (1 – 5)
1 – Very Low	Adversary would have no level of interest in the asset
2 – Low	Adversary would have some degree of interest in the asset
3 – Medium	Adversary would have a moderate degree of interest in attacking the asset
4 – High	Adversary would have a high degree of interest in the asset
5 – Very High	Adversary would have a very high degree of interest in the asset

Figure 3.14—Description of Step 3 and Substeps

Step	Task
Step 3: Vulnerability Analysis	
3.1 Define scenarios and evaluate specific consequences	Use scenario-analysis and/or use asset-based analysis to document the adversary's potential actions against an asset.
3.2 Evaluate effectiveness of existing security measures	Identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.
3.3 Identify vulnerabilities and estimate degree of vulnerability	Identify the potential vulnerabilities of each critical asset to applicable threats or adversaries. Estimate the degree of vulnerability of each critical asset for each threat-related undesirable event or incident and thus each applicable threat or adversary.

Step 3.1—Define Scenarios and Evaluate Specific Consequences

Each asset in the list of critical target assets from Step 2 is reviewed in light of the threat assessment, and the relevant threats and assets are paired in a matrix or other form of analysis, as shown in Attachment 1—Steps 3 – 5—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form. The importance of this step is to develop a design basis threat statement for each facility.

Once the SVA Team has determined how a malevolent event can be induced, it should determine how an adversary could execute the act.

The action in the Scenario-based approach follow the SVA method as outlined in Chapter 3. To establish an understanding of risk, scenarios can be assessed in terms of the severity of consequences and the likelihood of occurrence of security events. These are qualitative analyses based on the judgment and deliberation of knowledgeable team members.

Step 3.2—Evaluate Effectiveness of Existing Security Measures

The SVA Team will identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.

Step 3.3—Identify Vulnerabilities and Estimate Degree of Vulnerability

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and the subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices.

For each asset, the vulnerability or difficulty of attack is considered using the definitions shown in Figure 3.15.

The Scenario-based approach is identical to the Asset-based approach in the beginning, but differs in the degree of detailed analysis of threat scenarios. The scenario-based approach uses a more detailed analysis strategy and brainstorms a list of scenarios to understand how the undesired event might be accomplished. The scenario-based approach begins with an onsite inspection and interviews to gather specific information for the SVA Team to consider.

The following is a description of the approach and an explanation of the contents of each column of the worksheet in Attachment 1—Steps 3 – 5 Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form.

Figure 3.15—Vulnerability Rating Criteria

Vulnerability Level	Description
5 – Very High	Indicates that there are no effective protective measures currently in place to Deter, Detect, Delay, and Respond to the threat and so an adversary would easily be capable of exploiting the critical asset.
4 – High	Indicates there are some protective measures to Deter, Detect, Delay, or Respond to the asset but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the asset.
3 – Medium	Indicates that although there are some effective protective measures in place to Deter, Detect, Delay, and Respond, there isn't a complete and effective application of these security strategies and so the asset or the existing countermeasures could likely be compromised.
2 – Low	Indicates that there are effective protective measures in place to Deter, Detect, Delay, and Respond, however, at least one weakness exists that an adversary would be capable of exploiting with some effort to evade or defeat the countermeasure given substantial resources.
1 – Very Low	Indicates that multiple layers of effective protective measures to Deter, Detect, Delay, and Respond to the threat exist and the chance that the adversary would be able to exploit the asset is very low.

The SVA Team devises a scenario based on their perspective of the consequences that may result from undesired security events given a postulated threat for a given asset. This is described as an event sequence including the specific malicious act or cause and the potential consequences, while considering the challenge to the existing countermeasures. It is conservatively assumed that the existing countermeasures are exceeded or fail in order to achieve the most serious consequences, in order to understand the hazard. When considering the risk, the existing countermeasures need to be assessed as to their integrity, reliability, and ability to deter, detect, and delay.

In this column the type of malicious act is recorded. As described in Chapter 2, the four types of security events included in the objectives of a SVA at a minimum include:

1. Theft/Diversion of material for subsequent use as a weapon or a component of a weapon
2. Causing the deliberate loss of containment of a chemical present at the facility
3. Contamination of a chemical, tampering with a product, or sabotage of a system
4. An act causing degradation of assets, infrastructure, business and/or value of a company or an industry.

Given the information collected in Steps 1 – 3 regarding the site's key target assets, the attractiveness of these targets, and the existing layers and rings of protection, a description of the initiating event of a malicious act scenario may be entered into the Undesired Event column. The SVA team brainstorms the vulnerabilities based on the information collected in Steps 1 – 3. The SVA team should brainstorm vulnerabilities for all of the malicious act types that are applicable at a minimum. Other scenarios may be developed as appropriate.

Completing the Worksheet

The next step is for the team to evaluate scenarios concerning each asset/threat pairing as appropriate. The fields in the worksheet are completed as follows:

1. **Asset:** The asset under consideration is documented. The team selects from the targeted list of assets and considers the scenarios for each asset in turn based on priority.
2. **Security Event Type:** This column is used to describe the general type of malicious act under consideration. At a minimum, the four types of acts previously mentioned should be considered as applicable.
3. **Threat Category:** The category of adversary including terrorist, activist, disgruntled employee, etc.
4. **Type:** The type of adversary category whether (I) – Insider, (E) – External, or (C) – Colluded threat.
5. **Undesired Act:** A description of the sequence of events that would have to occur to breach the existing security measures is described in this column.
6. **Consequences:** Consequences of the event are analyzed and entered into the Consequence column of the worksheet. The consequences should be conservatively estimated given the intent of the adversary is to maximize their gain.
   It is recognized that the severity of an individual event may vary considerably, so SVA teams are encouraged to understand the expected consequence of a successful attack or security breach.
7. **Consequences Ranking:** Severity of the Consequences on a scale of 1 – 5 as shown in Figure 3.8. The severity rankings are assigned based on a conservative assumption of a successful attack.

8. **Existing Countermeasures:** The existing security countermeasures that relate to detecting, delaying, or deterring the adversaries from exploiting the vulnerabilities may be listed in this column. The countermeasures have to be functional (i.e., not bypassed or removed) and sufficiently maintained as prescribed (i.e., their ongoing integrity can be assumed to be as designed) for credit as a countermeasure.
9. **Vulnerability:** The specific countermeasures that would need to be circumvented or failed should be identified.
10. **Vulnerability Ranking:** The degree of vulnerability to the scenario rated on a scale of 1 – 5 as shown in Figure 3.15.
11. **L(ikelihood):** The likelihood of the security event is assigned a qualitative ranking in the likelihood column. The likelihood rankings are generally assigned based on the likelihood associated with the entire scenario, assuming that all countermeasures are functioning as designed/intended. Likelihood is a team decision and is assigned from the Likelihood scale based on the factors of Vulnerability, Attractiveness, and Threat for the particular scenario considered.
12. **R(isk):** The severity and likelihood rankings are combined in a relational manner to yield a risk ranking. The development of a risk-ranking scheme, including the risk ranking values is described in Step 4.
13. **New Countermeasures:** The recommendations for improved countermeasures that are developed are recorded in the New Countermeasures column.

3.6 STEP 4: RISK ANALYSIS/RANKING

In either the Asset-based or the Scenario-based approach to Vulnerability Analysis, the next step is to determine the level of risk of the adversary exploiting the asset given the existing security countermeasures. Figure 3.16 lists the substeps.

The scenarios are risk-ranked by the SVA Team based on a simple scale of 1 – 5. The risk matrix shown in Figure 3.17 could be used to plot each scenario based on its likelihood and consequences. The intent is to categorize the assets into discrete levels of risk so that appropriate countermeasures can be applied to each situation.

Note: For this matrix, a Risk Ranking of "5 x 5" represents the highest severity and highest likelihood possible.

3.7 STEP 5: IDENTIFY COUNTERMEASURES:

A Countermeasures Analysis identifies shortfalls between the existing security and the desirable security where additional recommendations may be justified to reduce risk. In assessing the need for additional countermeasures, the team should ensure each scenario has the following countermeasures strategies employed:

- **DETER** an attack if possible
- **DETECT** an attack if it occurs
- **DELAY** the attacker until appropriate authorities can intervene
- **RESPOND** to neutralize the adversary, to evacuate, shelter in place, call local authorities, control a release, or other actions.

The SVA Team evaluates the merits of possible additional countermeasures by listing them and estimating their net effect on the lowering of the likelihood or severity of the attack. The team attempts to lower the risk to the corporate standard.

Figure 3.16—Description of Step 4 and Substeps

Step	Task
Step 4: Risk Assessment	
4.1 Estimate risk of successful attack	As a function of consequence and probability of occurrence, determine the relative degree of risk to the facility in terms of the expected effect on each critical asset (a function of the consequences or impacts to the critical functions of the facility from the disruption or loss of the critical asset, as evaluated in Step 1) and the likelihood of a successful attack (a function of the threat or adversary, as evaluated in Step 2, and the degree of vulnerability of the asset, as evaluated in Step 3).
4.2 Prioritize risks	Prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks.

Figure 3.17—Risk Ranking Matrix

		SEVERITY				
LIKELIHOOD		**5**	**4**	**3**	**2**	**1**
	5	High	High	High	Med	Med
	4	High	High	Med	Med	Low
	3	High	Med	Med	Low	Low
	2	Med	Med	Low	Low	Low
	1	Med	Low	Low	Low	Low

Figure 3.18—Description of Step 5 and Substeps

Step	Task
Step 5: Countermeasures Analysis	
5.1 Identify and evaluate enhanced countermeasures options	Identify countermeasures options to further reduce the vulnerabilities and thus the risks while considering such factors as: • Reduced probability of successful attack • The degree of risk reduction provided by the options • The reliability and maintainability of the options • The capabilities and effectiveness of these mitigation options • The costs of the mitigation options • The feasibility of the options Rerank to evaluate effectiveness.
5.2 Prioritize potential enhancements	Prioritize the alternatives for implementing the various options and prepare recommendations for decision makers

3.8 FOLLOW-UP TO THE SVA

The outcome of the SVA is:

- the identification of security vulnerabilities;
- a set of recommendations (if necessary) to reduce risk to an acceptable level.

The SVA results should include a written report that documents:

- The date of the study;
- The study team members, their roles and expertise and experience;
- A description of the scope and objectives of the study;
- A description of or reference to the SVA methodology used for the study;
- The critical assets identified and their hazards and consequences;
- The security vulnerabilities of the facility;
- The existing countermeasures;
- A set of prioritized recommendations to reduce risk.

Once the report is released, it is necessary for a resolution management system to resolve issues in a timely manner and to document the actual resolution of each recommended action.

Attachment 1—Example SVA Methodology Forms

The following four forms can be used to document the SVA results. Blank forms are provided, along with a sample of how each form is to be completed. Other forms of documentation that meet the intent of the SVA guidance can be used.

Step 1: Critical Assets/Criticality Form		
Facility Name:		
Critical Assets Form		
Critical Assets	**Criticality/Hazards**	**Asset Severity Ranking**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

Step 2: Threat Assessment Form								
General Adversary Type	**Source**	**General Threat History**	**Site Specific Threat History**	**Potential Actions**	**Adversary Capability**	**Adversary Motivation/ Intent**	**Overall Assessment**	**Threat Ranking**
1. International Terrorists								
2. Domestic Terrorists								
3. Domestic Disgruntled Employee or Contractor								
4. Domestic Activists								

Step 2: Attractiveness/Target Ranking Form									
Facility Name:									
Critical Assets	**Function/Hazards/ Criticality**	**Asset Severity Ranking**	**Asset Attractiveness**						
			Foreign/Domestic Attractiveness Rationale	**A1**	**Employee/ Contractor Attractiveness Rationale**	**A2**	**Activist Attractiveness Rationale**	**A3**	**TR**
1.									
2.									
3.									
4.									
5.									
6.									

Step 3 – 5: Vulnerability Analysis/Risk Ranking/Countermeasures Form											
Facility Name:											
Critical Assets:											
Attractiveness:											
Security Event Type	**Threat Category**	**Type**	**Undesired Act**	**Consequences**	**S**	**Existing Countermeasures**	**Vulnerability**	**V**	**L**	**R**	**New Countermeasures**

Glossary of Terms[12]

Adversary: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

Alert levels: Describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different security measures may be implemented at each alert level based on the level of threat to the facility.

Asset: An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site.

Asset category: Assets may be categorized in many ways. Among these are:

- People
- Hazardous materials (used or produced)
- Information
- Environment
- Equipment
- Facilities
- Activities/Operations
- Company reputation

Benefit: Amount of expected risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities.

Capability: When assessing the capability of an adversary, two distinct categories need to be considered. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained, damaged, or destroyed.

Checklist: A list of items developed on the basis of past experience that is intended as a guide to assist in applying a standard level of care for the subject activity and to assist in completing the activity in as thorough a manner.

Consequences: The amount of loss or damage that can be expected, or may be expected from a successful attack against an asset. Loss may be monetary but may also include political, morale, operational effectiveness, or other impacts. The impacts of security events, which should involve those that are extremely severe. Some examples of relevant consequences in a SVA include fatality to member(s) of the public, fatality to company personnel, injuries to member(s) of the public, injuries to company personnel, large-scale disruption to public or private operations, large-scale disruption to company operations, large-scale environmental damage, large-scale financial loss, loss of critical data, and loss of reputation.

Cost: Includes tangible items such as money and equipment as well as the operational costs associated with the implementation of countermeasures. There are also intangible costs such as lost productivity, morale considerations, political embarrassment, and a variety of others. Costs may be borne by the individuals who are affected, the corporations they work for, or they may involve macroeconomic costs to society.

Cost-Benefit analysis: Part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of the tangible materials, and also the on-going operational costs associated with the countermeasure implementation.

Countermeasures: An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

Countermeasures analysis: A comparison of the expected effectiveness of the existing countermeasures for a given threat against the level of effectiveness judged to be required in order to determine the need for enhanced security measures.

Cyber security: Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

Delay: A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

Detection: A countermeasures strategy to that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

Deterrence: A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

Hazard: A situation with the potential for harm.

Intelligence: Information to characterize specific or general threats including the motivation, capabilities, and activities of adversaries.

Intent: A course of action that an adversary intends to follow.

Layers of protection: A concept whereby several independent devices, systems, or actions are provided to reduce the likelihood and severity of an undesirable event.

Likelihood of adversary success: The potential for causing a catastrophic event by defeating the countermeasures. LAS is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

Mitigation: The act of causing a consequence to be less severe.

Physical security: Security systems and architectural features that are intended to improve protection. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass.

Process Hazard Analysis (PHA): A hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

Response: The act of reacting to detected or actual criminal activity either immediately following detection or post-incident.

Risk: The potential for damage to or loss of an asset. Risk, in the context of process security, is the potential for a catastrophic outcome to be realized. Examples of the catastrophic outcomes that are typically of interest include an intentional release of hazardous materials to the atmosphere, or the theft of hazardous materials that could later be used as weapons, or the contamination of hazardous materials that may later harm the public, or the economic costs of the damage or disruption of a process.

Risk assessment: Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting vulnerability (V) and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for rank ordering of risks and thus establishing priorities for the application of countermeasures.

Safeguard: Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.4

Security layers of protection: Also known as concentric 'rings of protection', a concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as counter-surveillance, counterintelligence, physical security, and cyber security.

Security management system checklist: A checklist of desired features used by a facility to protect its assets.

Security plan: A document that describes an owner/operator's plan to address security issues and related events, including security assessment and mitigation options. This includes security alert levels and response measures to security threats.

Security Vulnerability Assessment (SVA): A SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. SVAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security and safety professionals. The determination

of risk (qualitatively) is the desired outcome of the SVA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

Target attractiveness: An estimate of the value of a target to an adversary based on the factors shown below. Experience has shown that, particularly for terrorist attacks, certain targets better accomplish the objectives of the adversaries than do others. Since the SVA is a risk-based analytical approach, consideration must be given to these factors in defining the threat and in determining the need for any enhanced countermeasures.

- Potential for mass casualties/fatalities
- Extensive property damage
- Proximity to national assets or landmarks
- Possible disruption or damage to critical infrastructure
- Disruption of the national, regional or local economy
- Ease of access to target
- Media attention or possible interest of the media
- Company reputation and brand exposure

Technical security: Electronic systems for increased protection or for other security purposes including access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

Terrorism: The FBI defines terrorism as, "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Threat categories: Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

Undesirable events: An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

Vulnerabilities: Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.

Abbreviations and Acronyms

A	Attractiveness
ACC	American Chemistry Council
AT	Target attractiveness
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
AWCS	Accidental Worst-Case Scenario
C	Consequence
CCPS¨	Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE)
CCTV	Closed Circuit Television
CEPPO	Chemical Emergency Preparedness and Prevention Office (USEPA)
CMP	Crisis Management Plan
CSMS	Chemical Security Management System
CW	Chemical Weapons
CWC	Chemical Weapons Convention
D	Difficulty of Attack
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	U. S. Department of Transportation
EHS	Environmental, Health, and Safety
EPA	U. S. Environmental Protection Agency
ERP	Emergency Response Process
EHS	Environmental, Health, and Safety
FBI	U. S. Federal Bureau of Investigation
FC	Facility Characterization
HI	Hazard Identification
HSAS	Homeland Security Advisory System
IPL	Independent Protection Layer
IT	Information Technology
LA	Likelihood of Adversary Attack
LAS	Likelihood of Adversary Success
LOPA	Layer of Protection Analysis
MARSEC	Maritime Security Levels
MOC	Management of Change
NPRA	National Petrochemical and Refiners Association
OSHA	Occupational Safety and Health Administration
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PSI	Process Safety Information
PSM	Process Safety Management (Also refers to requirements of 29 *CFR* 1910.119)
R	Risk
RMP	Risk Management Process (Also refers to requirements of EPA 40 *CFR* Part 68)
S	Severity of the Consequences
SOCMA	Synthetic Organic Chemical Manufacturers Association
SOP	Standard Operating Procedure
SVA	Security Vulnerability Assessment
T	Threat
TSA	Transportation Security Agency
V	Vulnerability
WMD	Weapons of Mass Destruction

APPENDIX A—SVA Supporting Data Requirements

SVA Methodology Supporting Data	
Category*	**Description**
A	Scaled drawings of the overall facility and the surrounding community (e.g., plot plan of facility, area map of community up to worst case scenario radius minimum)
A	Aerial photography of the facility and surrounding community (if available)
A	Information such as general process description, process flow diagrams, or block flow diagrams that describes basic operations of the process including raw materials, feedstocks, intermediates, products, utilities, and waste streams
A	Information (e.g., drawings that identify physical locations and routing) that describes the infrastructures upon which the facility relies (e.g., electric power, natural gas, petroleum fuels, telecommunications, transportation [road, rail, water, air], water/wastewater)
A	Previous security incident information
A	Description of guard force, physical security measures, electronic security measures, security policies
A	Threat information specific to the company (if available)
B	Specifications and descriptions for security related equipment and systems. Plot plan showing existing security countermeasures
B	RMP information including registration and offsite consequence analysis (if applicable, or similar information)
B	Most up-to-date PHA reports for processes considered targets
B	Emergency response plans and procedures (site, community response, and corporate contingency plans)
B	Information on material physical and hazard properties (MSDS)
B	Crisis management plans and procedures (site and corporate)
B	Complete a SVA chemicals checklist to determine whether the site handles any chemicals on the following lists:
C	• EPA Risk Management Program (RMP) 40 *CFR* Part 68;
C	• OSHA Process Safety Management (PSM) 29 *CFR* 1910.119;
C	• Chemical Weapons Convention, Schedule 2 and specifically listed Schedule 3 chemicals;
C	• FBI Community Outreach Program (FBI List) for WMD precursors;
C	• The Australia Group list of chemical and biological weapons.
C	Design basis for the processes (as required)
C	Unit plot plans of the processes
C	Process flow diagrams (PFDs) and piping and instrument diagrams (P&IDs) for process streams with hazardous materials
C	Safety systems including fire protection, detection, spill suppression systems
C	Process safety systems including safety instrumented systems (SIS), PLC's, process control systems
C	Operating procedures for start-up, shutdown, and emergency (operators may provide general overview of this information, with written information available as required)
C	Mechanical equipment drawings for critical equipment containing highly hazardous chemicals
C	Electrical one-line diagrams
C	Control system logic diagrams
C	Equipment data information
C	Information on materials of construction and their properties
C	Information on utilities used in the process
C	Test and maintenance procedures for security related equipment and systems

*Categories: A = Documentation to be provided to SVA team as much in advance as possible before arrival for familiarization;
B = Documentation to be gathered for use in SVA team meetings on site;
C = Documentation that should be readily available on an as-needed basis.

APPENDIX B—SVA Countermeasures Checklist

Appendix B Table of Contents

SVA Countermeasures Survey

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. This attachment contains checklists that are used to conduct the physical security portion of the survey. The Security Program Management Checklist is used to identify physical security measures that may be present to protect the entire facility or a critical asset at the facility. The remaining checklists are used to specifically evaluate the individual elements of the physical security system that are present. The conclusion of whether a particular element provides adequate protection is to be reported as part of the findings in the body of the SVA. A "set" of checklists should be completed for the facility as a whole and if appropriate, for each of the critical assets within the facility.

Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Instructions: This checklist identifies the physical security elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.	

Physical Security System Element	Element Present		COMMENTS
	Yes	No	
Perimeter Barriers			
Building Barriers			
Intrusion Detection			
Access Controls			
Security Force			

IDENTIFICATION OF PROCESS SAFETY SYSTEMS

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Instructions: This checklist identifies the process safety elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.	

Process Safety System Element	Element Present		COMMENTS
	Yes	No	
Hardening Processes			
Emergency Response			
Chemical Detection			
Fire Detection			
Fire Suppression			

SECURITY PROGRAM MANAGEMENT	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Security Organization	
1. Is there a senior level security working group with representatives from each major office or department to establish security policies (including physical security, operations security, and infrastructure interdependencies security) and integrate them across all elements of the organization? • If there is a senior level security working group, describe the membership, the lines of communication, and any scheduled periodic meetings to resolve security issues. • If there is not such a group, how are security policies established?	
2. Is there a security office that is responsible for implementing security policies and procedures (including physical security, operations security, and infrastructure interdependencies security)? • If there is a security office, where does it report in the organization, how many people are in the office, and are resources adequate? Also describe any training received. • If there is not such an office, how are security policies implemented?	
(b) Security Plans and Policies	
3. Is there a mission statement describing the physical security, operations security, and infrastructure security programs?	
4. Is there a formal security plan and statement of security policies? If there is, describe it including how it is communicated to employees.	
5. Is there a formal threat definition and assessment statement? If there is, describe it including how it is communicated to employees.	
(c) Security Resources	
1. Are the resources (budget and staffing) applied to security (including physical security, operations security, and infrastructure interdependencies security) considered adequate?	
2. Do security personnel feel that they have adequate training to accomplish their functions?	
(d) Senior Management Security	
1. Is there an executive protection program for senior executives/managers? If there is such a program, describe it.	
2. Is public information on senior executives/managers controlled? If it is, describe how it is controlled.	
(e) Security Audits	
1. Is there a regular security assessment or audit? If there is, describe how it is done, by whom, and how frequently.	

2. Has the most recent audit indicated any weaknesses? Summarize the results of the audit, particularly any weaknesses identified.	
3. Have any corrective measures been implemented recently? Describe them.	
(f) Handling of Sensitive Information	
1. How is sensitive information identified and marked?	
2. Who has access to sensitive security information?	
3. How is sensitive information protected, stored, accessed, transmitted, and destroyed?	
4. How do senior executives/managers protect sensitive security information?	
(g) Internal Communications	
1. How does management provide security information to employees at the site?	
2. Describe the process for obtaining feedback from employees on security related issues.	

THREAT DETECTION AND EVALUATION CAPABILITIES	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
(a) Threat Analysis Working Group	
1. Is the organization a member of a local threat analysis working group? Describe the group	
2. If the organization is a member of such a group, list the organizations that participate in the working group (e.g., local, county, state, and federal agencies, the military).	
3. Are there other industry partners participating in the working group? Describe them.	
4. Are active efforts being made to recruit other meaningful participants into the working group? Describe the efforts.	
5. Do the participants in the working group have management support, requirements, and funding to participate? Describe the situation.	
6. Are the members of the working group willing participants and do they work against bureaucratic obstacles that may prevent the success of the group? Describe the situation.	
7. Do the members of the working group have the authority to share information with other members of the group? Describe the situation.	
8. Have the members of the working group been given appropriate U.S. government clearances to share in threat information? Describe the situation.	
9. Do the members of the working group have access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc., (ANSER), FBI-sponsored InfraGuard, Carnegie Mellon University's CERT¨, and other information system security warning notices? List the threat information systems they use.	
10. Indicate the frequency and regularity of the working group meetings.	
11. Do the members of the working group have processes in place to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses, other working groups in the area)? Describe these processes.	
12. Do members of the working group have the ability to initiate information-gathering requests back into the field environment? Describe the capability.	
13. Are the threat statements developed by the working group specific to the organization or the industry, versus general nationwide warnings? Describe the process for gathering these statements.	

14. Do some members of the working group conduct scheduled meetings with the public to discuss concerns and observations? Describe these interactions.	
15. Do the members of the working group know what the critical assets of the organization are? Describe the extent of their knowledge.	
16. Do the members of the working group understand industry interdependencies and work with other industry members to address these potential concerns? Describe the extent of these interactions.	
17. What are the roles and responsibilities of the working group members during response and recovery activities?	
(b) Organization's Response to Threat Updates	
1. Does senior management support and/or participate in the threat analysis working group? Describe the extent of the support/participation.	
2. Does the organization receive as-needed threat briefings from local, state, and federal agencies? Describe the nature and extent of the briefings.	
3. Does the organization have the ability to distribute organization-specific threat warnings in real time? Describe the process.	
4. Does the organization have the ability to augment security programs based on threat updates? Describe the process.	
5. Does the organization conduct historical trending analysis for security events (both planned and actual) and implement security activates to mitigate them? Describe the analysis.	
6. Does the organization create possible threat scenarios based on input from the threat analysis working group and conduct related security exercises? Describe the exercises.	

PERIMETER BARRIERS—FENCES, GATES	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Fences	
1. Characterize fence construction and rate the level of security it provides as low, moderate to high, or other (specify). • Low: no fence or only a 6-foot chain-link fence. • Moderate to high: 8-foot chain-link fence with outriggers, 10 to 12-foot chain-link fence, or over 12-foot chain-link fence with outriggers.	
2. Characterize fence signage as no signs, posted "No Trespassing," or other (specify).	
3. Characterize the fence alarm system as no alarms, fence sensors (taut wire, vibration, strain, electric field, or multiple sensors), or other (specify).	
4. Fence area: • Is the fence within 2 inches of firm hard ground? • Is the fence line clear of vegetation, trash, equipment, and other objects that could impede observation? • Is the area free of objects that would aid in traversing the fence? • Is physical protection installed for all points where utilities (e.g., electric power lines, natural gas pipelines, telecommunication lines, water supply, storm sewers, drainage swells) intersect the fence perimeter?	
5. How is the fence protected from vehicles (aircraft cable, concrete barriers or median, guard rails, steel posts, a ditch, crash I-beams, train barrier, or other [specify])?	
6. Fence illumination: • Is there security lighting for the fences? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	
(b) Gates	
1. Characterize the gates as no gate closure, vehicle bar, chain-link fence, or other (specify).	
2. Characterize the gate locks as no lock, lock not used, gate unlocked, gate attended by personnel when unlocked, ID actuated lock, padlock, or other (specify).	
3. How is access to gate keys controlled?	
4. Gate lighting: • Describe the security lighting for the gates. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	
(c) Vehicle Barriers	
1. Characterize vehicle barriers as none, a vehicle bar, blocked by vehicle when gate open, hydraulic wedge, or other (specify).	

BUILDING BARRIERS—WALLS, ROOF/CEILING, WINDOWS, DOORS	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Walls	
2. Characterize wall construction and rate the level of security wall provide as low, moderate, or high. • Low: chain-link mesh, 16-gauge metal, wood studs and dry wall, wood studs and plywood, or other (specify). • Moderate: clay block, 8-inch hollow block, 8-inch filled block, or other (specify). • High: 8-inch filled rebar block, 12-inch filled rebar block, 2-inch precast concrete tees, 4-inch reinforced concrete, 8-inch reinforced concrete, 12-inch reinforced concrete, 24-inch reinforced concrete, or other (specify).	
3. Do the walls extend from the floor to the structural ceiling?	
(b) Roof/Ceiling	
1. Characterize the roof material and rate the level of security it provides as low, moderate, or high. • Low: 20-gauge metal with insulation, ½-inch wood, or other (specify). • Moderate: 20-gauge metal built-up roof, concrete built-up roof with T-beams, or other (specify). • High: 5-½-inch concrete roof, 8-inch concrete roof, 3-foot earth cover, 3-foot soil/cement/earth cover, or other (specify).	
2. Does the interior drop ceiling extend beyond the structural walls?	
(c) Windows	
1. Characterize the window materials and rate the level of security they provide as low or moderate. • Low: standard windows or other (specify). • Moderate: 9-gauge expanded mesh, ½-inch diameter x 1-½-inch quarry screen, ½-inch diameter bars with 6-inch spacing, $^{3}/_{16}$-inch x 2-½-inch grating, or other (specify).	
2. Characterize the window alarms (for windows that would be accessible by foot or ladder) as none, vibration sensor, glass breakage sensor, conducting tape, grid mesh, multiple sensors, or other (specify).	

(d) Doors	
1. Characterize door materials and rate the level of security they provide as low, moderate, or high. • Low: wood, 9-gauge wire mesh, hollow-core metal, no lock/hinge, or other (specify). • Moderate: hollow-core metal, tempered-glass panel, security-glass panel, half-height turnstile, or other (specify). • High security: ½-inch steel plate, turnstile – aluminum, Class V or VI vault, or other (specify).	
2. Characterize the door locks and rate the level of security they provide as low, moderate, or high. • Low: none, lock not used, or other (specify). • Moderate: door unlocked, attended by personnel when unlocked, ID actuated lock, padlock, keyed cylinder lock, combination lock, mechanically coded lock, or other (specify). • High: electronically coded lock, two-person rule lock system, lock inaccessible from the door exterior, or other (specify).	
3. How is access to the keys for the door locks controlled?	
4. Door Alarms: • Is door position monitored? • Indicate the type of door penetration sensor (vibration, glass breakage, conducting tape, grid mesh, or other [specify]).	

INTRUSION DETECTION	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Intrusion Sensors (If Applicable)	
1. Characterize the exterior intrusion sensors as seismic buried cable, electric field, infrared, microwave, video motion, or other (specify).	
2. Characterize the interior intrusion sensors as sonic, capacitance, video motion, infrared, ultrasonic, microwave, or other (specify).	
(b) Intrusion Alarm Deployment (If Applicable)	
1. Characterize intrusions alarm deployment in terms such as: • continuously monitored, • positioned to prevent gaps in coverage, • detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris), • tamper and system problem indicators provided, • compensatory measures employed when alarms are not operating, • backup power provided, and • other (specify).	
(c) Intrusion Alarm Assessment	
1. Characterize the assessment of intrusion alarms as not assessed, closed circuit TV, automatic deployment of protective force, or other (specify).	

CLOSED CIRCUIT TELEVISION	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(a) CCTV	
1. Describe the current CCTV system in use at the site.	
2. Characterize cameras in use and what asset(s) the cameras cover (PTZ, Autodome type, Fixed, Day/Night)	
3. Who monitors the CCTV cameras (Operations and/or Security) and what are the protocols for camera operation?	
4. Describe the policy for review of information recorded on CCTV system.	
5. Describe the preventive maintenance program for the CCTV system.	

ACCESS CONTROL	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(a) Personnel Access	
1. Characterize access point control as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the identification check process as none in place, casual recognition, credential check (e.g., drivers license, passport, state ID), picture badge, PIN, exchange badge, retinal scan, hand geometry, speech pattern, signature dynamics, fingerprint, or other (specify).	
3. Characterize the organization's badging policy in terms such as no badging policy, visitor badges required, badge issuance and control procedures in place (describe), and badges show permission to access specific areas (describe).	
(b) Vehicle Access	
1. Characterize vehicle access point controls as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the vehicle access identification process as none in place, vehicle stickers, vehicle stickers with personnel identification, automated system (describe), or other (specify).	
3. Describe the vetting process for incoming/outgoing bulk shipments of items by vehicle. Are deliveries scheduled or are is a list of drivers provided prior to delivery.	
(c) Contraband Detection	
1. Characterize item and vehicle search procedures as none, cursory, or detailed	
2. Is there a policy for incoming/outgoing drivers that report the possession of weapons? If so describe the policy/procedure.	
(d) Access Point Illumination	
1. Access Point Illumination: • Is there security lighting for the access points? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	

SECURITY FORCE	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Protective Force	
1. Specify the size of the protective force in terms or total number and the number on duty during working hours, non-working hours, and weekends/holidays.	
2. Specify the equipment available to the protective force such as uniforms; vehicles (specify number); weapons (describe); communications devices (describe); and other equipment (describe).	
3. Describe the training of the protective force. Specifically, describe the initial training, any continuing training (e.g., on-the-job), and drills and exercises.	
4. Describe the organization of the protective force. Specifically, describe the command structure, their mission as defined, any established policies and procedures, and established emergency response plans.	
5. Are there provisions for a back-up force (e.g., recalling off-duty personnel)? Describe the provisions in place.	
6. Protective Force Command Center: • Is there a protective force command and control center? Describe it. • Is there a backup center? Describe it.	
7. Are protective force operations disguised to prevent intelligence about the facility from being inadvertently released? Describe how this is done.	
8. Describe protective force procedures for responding to alarms.	
9. Does the protective force provide security escort for visitors? Describe the nature of the escort.	
(b) Local Law Enforcement Agencies	
1. Describe the interaction of the protective force with local law enforcement agencies in terms of memoranda of agreement or other agreements in place (describe), protection responsibilities defined (describe), communication procedures developed (describe), and participation in drills and exercises.	
2. What is the approximate response time for local law enforcement personnel?	

INFORMATION, COMPUTER, NETWORK, and INTELLECTUAL PROPERTY SECURITY	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Information, Computer, Network, and Intellectual Property Security	
1. Have steps been taken to protect technical and business information that could be of use to potential adversaries (sometimes referred to as operational security or OPSEC)?	
2. Have the documentation/computer files that need to be protected for confidentiality been systematically identified and regularly backed-up?	
3. Is sensitive information in research and development and laboratory areas safeguarded against inadvertent disclosure?	
4. Is sensitive information in maintenance areas safeguarded against inadvertent disclosure?	
5. Are computers as well as disks, tapes, and other media adequately secured physically from theft?	
6. Are procedures followed to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries?	
7. If the content of radio communications cannot be restricted for operational reasons, have they been voice-encrypted?	
8. Are user authorizations granted on the basis of "need to know," "least access," and "separation of functions" rather than position or precedent (note: this has to be balanced against the process safety concepts of employee access to process safety information and employee participation)?	
9. Are appropriate procedures followed for protecting and destroying sensitive documents that could provide key information on critical process operation or vulnerabilities?	
10. Is the computer/server room secured?	
11. Is the computer/server room on the second floor (to protect it from flooding and to reduce the likelihood of theft), and away from outside walls?	
12. Is the computer/server room equipped with adequate communications capability?	
13. Is access to the computer/server room limited to only authorized personnel who need entry?	
14. Are appropriate hardware, software, and procedural techniques used for protecting computers and networks, such as:	
a. Firewalls?	
b. User ID?	

c. Password controls, including the regular changing of passwords?	
d. Encryption?	
15. Virus protection?	
16. Are computer transaction histories periodically analyzed to look for irregularities that might indicate security breaches?	
17. Is Internet access disabled in all application software or operating systems that are pre-packaged?	
18. Are measures in place to control access to or otherwise secure process-specific operating information (e.g., including diagrams, procedures, control loop/DCS information), both electronic and hardcopy versions?	
19. Are process control systems protected from external manipulation (e.g., hacking into control system to operate equipment or delete or alter software codes)?	
20. Is access to process control systems via the Internet or Intranet been restricted? If access is allowed, is the access allowed only to the absolute minimum number of personnel necessary, using user ID, password, separate authentication, and encryption controls as appropriate?	
21. Are temporary passwords restricted from use except for new employees, or when a password is forgotten or is inactive?	
22. Are vendor-supplied passwords changed immediately after installation?	
23. Do users have screen saver with password available and in use when leaving computers on and unattended?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Hardening Processes	
1. Have existing security countermeasures been designed using the concept of rings of protection? Are the critical assets that may qualify as attractive targets at the center of concentric rings of layered protective features?	
2. Have process and systems been designed using the concept of layers of protection? Are there adequate independent protective layers that would detect, prevent, or mitigate a release of hazardous materials?	
3. Are critical process areas and equipment protected with traffic barriers, bollards, dikes, or other measures (e.g., diversionary structures that prevent vehicles from accelerating along a clear path to the process/equipment) to prevent ramming with vehicles?	
4. Are process "unit roads or streets" (i.e., roadways that provide access into specific process areas) provided with gates and, if so, are they securely closed when not in use (these gates may help limit direct vehicular access to critical equipment)?	
5. Are vehicles (except necessary material transport vehicles and/or authorized plant vehicles) prohibited from parking near critical process equipment (300 feet is considered a minimum distance)?	
6. Are full tank trailers or rail cars containing highly hazardous materials (i.e., those materials that could be targeted by terrorists) stored away from fence lines or perimeter areas to reduce their vulnerability to attack?	
7. Are full tank trailers or rail cars containing flammable or explosive materials stored away from critical process areas and equipment to prevent propagation of effects to critical processes?	
8. Are critical processes or equipment, such as tanks storing highly hazardous materials, protected from explosion or fire at adjacent processes (e.g., blast walls)?	
9. Is good housekeeping practiced in critical process areas and are trash dumpsters or receptacles located away from critical processes and equipment (trash dumpsters and poor housekeeping may make it easier to hide a bomb)?	
10. Are doors to interior buildings (e.g., process buildings) and control rooms locked or otherwise secured, where appropriate?	

11. Are hinge pins on doors to critical process areas on the inside of the door? (Note: May not be possible and still maintain easy egress in fire/emergency situations—doors must open out.)	
12. Are critical process areas surrounded with locked and secure fencing (in addition to site perimeter fencing) or located within locked buildings? (Note: Locked and secured fencing or buildings may create confined space issues.)	
13. If critical process areas are not surrounded by fencing or within buildings or if infeasible to do so, are the processes patrolled or monitored continuously by security personnel?	
14. Are highly reactive materials (e.g., water-reactive chemicals) stored in a location and manner that minimizes the potential for intentional contamination (e.g., stored in locked building away from water hose connections, situated away from pipelines/connections with potential incompatible chemicals)?	
15. Are key valves, pumps, metering stations, and open-ended lines on critical processes, especially those in remote or uncontrolled/ unrestricted areas, locked closed, located in locked secure structures (e.g., pump house), surrounded by locked secure fencing, and/or constructed of heavy-duty, tamper-resistant materials?	
16. Are ingredients for products potentially targeted for contamination unloaded, stored, transferred, and added to the process in a manner that is monitored and checked?	
17. Can exposed/remote equipment on critical processes feasibly be re-located to more secure/less vulnerable locations?	
18. Can critical process equipment that is highly recognizable from the ground and/or site perimeter be made less recognizable? (Note: This must be balanced against emergency responders need to readily identify equipment)	
19. Can critical processes or equipment be recognized readily from the air (consult aerial photos, if available) and, if so, can they be made less recognizable? (Note: This must be balanced against safety and code issues, such as painting of certain storage tanks in light colors.)	
(b) Reducing the Quantity and Hazard of a Release from a Malicious Act	
1. Has a review of site utility systems been conducted to identify and assess vulnerability of utilities that are essential to safe operation and shutdown of critical processes? Examples of possible critical utilities are:	

a. Electrical power	
b. Cooling water	
c. Compressed air	
d. Natural gas or other fuels	
e. Steam	
f. Nitrogen or other inert gases	
g. Secondary containment (drainage and sewer systems)	
h. Communications systems	
2. Are utility areas that can affect critical processes appropriately secured and monitored? (e.g., cooling water systems and agitation systems on reactive chemical processes that may be particularly important)	
3. Where appropriate, has safe and rapid manual shutdown capability been provided for critical processes and utilities?	
4. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, is the operating status of the utilities monitored and/or to alert personnel (e.g., an alarm sounds when cooling water flow is lost or reduced below critical levels)?	
5. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, are feed systems interlocked to agitation, cooling systems, and other appropriate utilities in the event of loss of those utilities or systems?	
6. Are appropriate back-up power supplies available for critical processes to allow a safe shutdown? (Note: UPS can be compromised by adversaries.)	
7. In the event of loss of power or pneumatics, do valves and other equipment fail to a safe position in critical processes?	
8. Are container storage areas secured or otherwise monitored, especially those outside of process buildings or in remote areas? (Note: A fire or explosion involving multiple containers can lead to smoke/combustion by-products that present offsite hazards and can serve as a diversion or a "statement.")	
9. Have storage and process inventories of hazardous chemicals been reduced to the extent practicable?	
10. Where appropriate, are critical processes containing highly hazardous chemicals "segmented" (either automatically or via manual action) to prevent release of the majority of process contents (i.e., only the quantity in the compromised "segment" would be released)?	
11. Are pipelines containing highly hazardous materials equipped with low-pressure interlock systems that shut valves or take other action to minimize the release quantity?	

12. Are open-ended lines or other lines or vessel drain systems on critical processes equipped with excess flow valves?	
13. Where appropriate, are hazardous materials being procured in smaller containers instead of maintaining large inventories in a single vessel?	
14. Has a review been conducted to determine if hazardous materials can be purchased and used in a less hazardous form? (Note: This may be particularly applicable to solvents/carriers and waste or water treatment chemicals.)	
15. If materials can be purchased and used in less hazardous forms, is this approach being addressed in an expedited manner?	
16. Has the feasibility and merit of storing large inventories of highly hazardous materials in underground tanks or other systems (e.g., aboveground vaults) that would limit the release rate been evaluated? (Note: This must be balanced against environmental concerns and other liabilities.) If found to be of merit, are plans in place to pursue this approach?	
17. Where appropriate and feasible, are tanks, vessels, and tank trailers/rail cars disconnected from delivery or transfer piping when not in use? (Note: The piping may be more vulnerable than the vessel.)	
(c) Mitigating a Release from a Malicious Act	
1. Are appropriate passive mitigation systems in-place for addressing large volume releases from critical processes?	
2. Have passive mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
3. Has passive leak-limiting technology been used where possible (e.g., gaskets resistant to blowout, excess flow valves, etc.)?	
4. Are appropriate active mitigation systems in-place for addressing large volume releases at critical processes?	
5. Have active mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
6. Are key control valves, pumps, and other equipment associated with active mitigation systems been locked or secured in operational/ready positions or located within secure structures?	
7. Has expanding the areas of the site where potential ignition sources are limited or eliminated (e.g., expanding the area of site subject to Class I/Div 1 or 2 electrical classification) been evaluated?	

(d) Emergency Response, Crisis Management, and Community Coordination	
1. Is the site's emergency response plan updated for current personnel and organizational functions?	
2. Do emergency plans address security worst case events, or events that are equivalent to security worst case events?	
3. Do emergency plans address malicious acts, especially responder actions in the event of a suspected terrorist/saboteur attack?	
4. Do emergency shutdown procedures address actions to take in the event of catastrophic releases or other terrorist-type event to safely shutdown the process and limit the release? If not, are shutdown procedures being reviewed and updated accordingly?	
5. Does the crisis management plan account for events such as:	
a. Bomb threats?	
b. Elevated homeland security warning status?	
c. Civil disturbance?	
6. Are operating personnel trained in the above-referenced emergency shutdown procedures, especially where they have been updated to address catastrophic or terrorist events?	
7. Has emergency equipment stationed near critical processes (e.g., hose connections) been assessed for vulnerability to compromise and, where appropriate, secured, monitored, or otherwise protected?	
8. If responding to a malicious act, are emergency responders aware that secondary "sucker-punch" devices (i.e., additional incendiary/explosive devices) or effects may be present if flammables are released or explosions are involved?	
9. Are procedures in-place (and responders trained accordingly) to address preservation of evidence due to the area being considered a crime scene?	
10. Where other nearby targets may exist (especially those that may present a greater risk than processes at our site), are plans in place to coordinate with local responders to ensure that those targets are monitored or otherwise protected in the event of a potential "diversionary" attack on our site?	
11. Have plans been developed with adjacent or nearby industry and local officials to facilitate timely communication of suspicious activity between potentially concerned parties?	
12. Have evacuation and shelter-in-place plans been fully developed and coordinated with local offsite emergency responders?	
13. Have local residents and business been instructed on how to shelter-in-place?	

14. Are local police, fire departments, health care providers, and other emergency responders aware of the hazardous materials at the site?	
15. Are plans in place to communicate information to local offsite emergency responders and officials in the event of a release?	
16. Do periodic emergency drills address malicious acts or other security-related emergencies?	
17. Is there a drill/exercise critique system in place to assure that experience from drills and actual emergencies are incorporated into the emergency response plan?	

APPENDIX C— SVA Interdependencies and Infrastructure Checklist

Appendix C Table of Contents

INTERDEPENDENCIES TABLES

INTERNAL AND EXTERNAL INFRASTRUCTURES TO BE INCLUDED

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

(Note: Not all infrastructures supporting each asset/facility need to be included in this survey. Only those infrastructures that are important to the asset's/facility's ability to continue to carry out its critical functions and activities need be considered in detail. In addition, the time and resources allotted for the survey may limit the infrastructures that can be examined.)

INFRASTRUCTURE	YES	NO	RATIONALE FOR EXCLUSION/INCLUSION
Internal			
Electric Power Supply and Distribution System			
HVAC System			
Telephone System			
Microwave/Radio Communications System			
Intranet and E-mail System			
Computers and Servers			
Fire Suppression/ Fire Fighting System			
SCADA System			
Domestic Water System			
Industrial Water System			
Physical Security System			
Human Resources Support			
Financial System			
External			
Electric Power			
Natural Gas			
Petroleum Fuels			
Telecommunications			
Water and Wastewater			
Road Transportation			
Rail Transportation			
Air Transportation			
Water Transportation			

INFRASTRUCTURE OVERSIGHT AND PROCEDURES	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Infrastructure Oversight	
Does the facility have a central office or department (such as building management, plant services, facility management) that is responsible for overseeing all or most the infrastructures? Indicate the office/department and list the infrastructures for which they have responsibility and the extent of their responsibilities.	
What coordination or oversight role does the physical security office have in regards to the infrastructures that support critical functions or activities?	
(b) Infrastructure Procedures	
In general, are operating procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, their availability to relevant staff, and the extent to which they are regularly followed. (Note: details about procedures for specific individual infrastructures are addressed in the relevant checklists.)	
Are contingency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: Contingencies refer to situations brought about by a failure or disruption within an infrastructure or the infrastructures that support it.)	
If they exist, have the contingency procedures been tested and are they exercised regularly either as a part of normal operations as through specially designed drills? Describe the drills and their results.	
Are emergency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: Emergencies refer to situations brought about external stress on the facility such as high demands.)	
If they exist, have the emergency procedures been tested and are they exercised regularly through specially designed drills? Describe the drills and their results.	

INTERNAL ELECTRIC POWER SUPPLY AND DISTRIBUTION SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Primary Source of Electric Power	
If the primary source of electric power is a commercial source, are there multiple independent feeds? If so, describe the feeds and their locations.	
If the primary source of electric power is a system operated by the facility or asset, what type of system is it?	
If a facility operated primary electric generation system is used, what is the fuel or fuels used?	
If petroleum fuel is used, what quantity of fuel is stored on site for the primary electric generation system and how long it will last under different operating conditions?	
If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	
(b) Electric Distribution System	
Are the components of the electric system that are located outside of buildings (such as generators, fuel storage facilities, transformers, transfer switches) protected from vandalism or accidental damage by fences or barriers? If so, describe the type of protection and level of security it provides.	
Are the various sources of electric power and the components of the internal electric distribution systems such that they may be isolated for maintenance or replacement without affecting the critical functions of the asset/facility? If not, describe the limitations.	
Have any single points of failure been identified for the electrical power supply and distribution system? If so, list them and describe.	
(c) Backup Electric Power Systems	
Are there additional emergency sources of electric supply beyond the primary system (such as multiple independent commercial feeds, backup generators, uninterruptible power supply [UPSs])? If there are, describe them.	
If there is a central UPS, does it support all the critical functions of the asset/facility in terms of capacity and connectivity? Specify for how long it can operate on battery power and list any potentially critical functions that are not supported.	
If there is a backup generator system, does it support all the critical functions of the facility in terms of capacity and connectivity? Specify the fuel and list any potentially critical functions that are not supported.	
Is the fuel for the backup generator system a petroleum fuel? If yes, specify the quantity stored on site and how long it will last.	
If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	

INTERNAL HVAC SYSTEM
(Including Heating Plants and Cooling Towers)

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Primary HVAC System	
Can critical functions and activities dependent on environmental conditions continue without the HVAC system? If yes, specify which functions and for how long they can continue under various external weather conditions.	
Is the HVAC system that supplies the areas of the asset/facility where critical functions dependent on environmental conditions are carried out separate from or separable fromthe general asset/facility-wide HVAC system?	
(b) Supporting Infrastructures	
Does the HVAC system (or critical portion thereof) depend on the primary electric power supply and distribution system to supply electric power? Specify under what conditions and for how long.	
Besides or in addition to electric power, on what fuel or fuels does the HVAC system (or critical portion thereof) depend?	
If the HVAC system (or critical portion thereof) depends on natural gas, are there provisions for alternative fuels during a natural gas outage? Specify the fuel and how long the HVAC system can operate on it.	
If the HVAC system (or critical portion thereof) depends on petroleum fuels for adequate operation, specify the type of fuel and how long the HVAC system can operate on the fuel available on site.	
If the HVAC system (or critical portion thereof) depends on petroleum fuels, are arrangements and contracts in place for resupply and management of the fuel?	
Does the HVAC system (or critical portion thereof) depend on water? If it does, specify if the water need is continuous or for make-up purposes only and the quantities/rates involved.	
If the HVAC system (or critical portion thereof) depends on water, is a backup supply in place such as well and pump, storage tank, or tank trucks? Specify how long the HVAC can operate on the backup water supply system.	
(c) Backup HVAC Systems	
Is there a separate backup to the HVAC system? If yes, describe the system and the energy and water supply systems it requires.	
Are there contingency procedures in place to continue with the critical functions and activities that take place at the asset/facility during an HVAC outage? If yes, briefly describe them.	
How long can the critical functions and activities at the asset/facility continue using the backup HVAC system or under the contingency procedures?	

INTERNAL TELEPHONE SYSTEMS
(Including Voice, FAX, and Data Transfer)

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Primary Telephone System	
What types of telephone systems are used within the asset/facility? Are there multiple independent telephone systems? Specify the types of systems, their uses, and whether they are copper-wire or fiber-optic based.	
If there are there multiple independent telephone systems within the asset/facility, is each one adequate to support the critical functions and activities? Indicate any limitations.	
If there are multiple (from independent systems) or redundant (from built-in backups) switches and cables, are they physically separated and isolated to avoid common causes of failure?	
Are the telephone switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify types of protection provided.	
(b) Data Transfer	
For large volume and high-speed data transfer within the asset/facility, is there a separate system of switches and cables within the asset/facility? Specify the type of system and whether it is copper-wire or fiber-optic based.	
If there is a separate system for large-volume and high-speed data transfer, are there redundant switches and cables? If yes, describe the situation.	
If there are redundant switches and cables, are they physically separated and isolated to avoid common causes of failure?	
Are the data-transfer switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify the types of protection provided.	
(c) Cellular/Wireless/Satellite Systems	
Are cellular/wireless telephones and pagers in widespread use within the asset/facility? If yes, briefly describe their uses.	
If cellular/wireless telephones and pagers are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.	
Are satellite telephones or data links in widespread use within the asset/facility? If yes, briefly describe their uses.	
If satellite telephones or data links are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.	

INTERNAL MICROWAVE/RADIO COMMUNICATIONS SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) On-site Fixed Components	
Are there multiple or redundant radio communications systems in place within the asset/facility? If yes, specify the types of systems and their uses.	
If there are multiple radio communications systems, is more than one system adequate to support all the critical functions and activities of the asset/facility? Specify any limitations.	
Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the radio communications systems? If yes, indicate under what conditions and for how long.	
Do the radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.	
Are the components of the system located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.	
(b) Mobile and Remote Components	
Are there mobile components to the radio communications system (such as on vehicles or vessels)? If yes, describe the mobile components.	
Are the mobile components of the radio communications system protected from vandalism or accidental damage by locked boxes or lockable vehicle cabs? Specify the types of protection and level of security they provide.	
Are there remote components to the radio communications system (such as relay towers)? If yes, describe them and their uses.	
Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.	
Are there environmental controls required for the remote components (such as heating, cooling)? If yes, describe them.	
Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.	
Is physical security provided for the remote components of the radio communications system? If yes, specify the types of security and the level of protection provided.	
Are there alarms at the remote components of the radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and the response procedure.	

INTERNAL INTRANET AND E-MAIL SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Contained within a Larger System	
Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's computers and servers? If yes, describe the dependence.	
Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's telephone system? If yes, describe the dependence.	
(b) Separate System	
If the asset's/facility's intranet and e-mail system is a separate system, are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the intranet and e-mail system? If yes, specify under what conditions and for how long.	
If the asset's/facility's intranet and e-mail system is a separate system, does it have its own backup electric power supply, such as local UPSs? If yes, specify the type and how long it can operate.	
If the asset's/facility's intranet and e-mail system is a separate system, does the asset's/facility's central HVAC system provide environmental control for important components or does it have its own independent environmental control system? If it has its own, specify the type.	
If the asset's/facility's intranet and e-mail system is a separate system, can it operate with a loss of all environmental control? If yes, specify for how long under various conditions.	
If the asset's/facility's intranet and e-mail system is a separate system, are there any backup environmental controls explicitly for the system? If yes, indicate the type of backup and the expected maximum duration of operation.	
If the asset's/facility's intranet and e-mail system is a separate system, is there special physical security provided for the important components? If yes, specify the type of security and the level of protection provided.	
If the asset's/facility's intranet and e-mail system is a separate system, is there special fire suppression equipment for the important components such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.	
If the asset's/facility's intranet and e-mail system is a separate system, are there special features or equipment in the area of the important components to limit flooding or water intrusion? If yes, indicate the precautions taken.	

If the asset's/facility's intranet and e-mail system is a separate system, are there alarms for the area of the important components for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.	
(c) Access	
Does the asset/facility have a backup or redundant intranet and e-mail system? If yes, describe the system and the amount of backup it provides.	
Do areas where critical functions and activities take place have multiple or redundant access to the intranet and e-mail system?	
If there are multiple access routes, is each one adequate to support the critical functions and activities? If not, specify any limitations.	

INTERNAL COMPUTERS AND SERVERS
(Including Mainframes, Firewalls, and Router Equipment)

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Electric Power Sources	
Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the computers and servers? If yes, indicate under what conditions and for how long.	
Do the computers and servers have their own backup electric power supply (such as local UPSs or generators)? If yes, specify the types of backup and how long they can operate.	
(b) Environmental Control	
Does the asset's/facility's central HVAC system provide environment control to the computer and server areas or do the computer and server areas have their own independent environmental control system? If they have their own system, specify the type.	
Can the computers and servers operate with a loss of all environmental control? If yes, specify for how long under various conditions.	
Are there any backup environmental controls explicitly for the computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.	
(c) Protection	
Is there special physical security provided for the computer and server areas? If yes, specify the type of security and the level of protection provided.	
Is there special fire suppression equipment in the computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type.	
Are there special features or equipment in the computer and server areas to limit flooding or water intrusion? If yes, describe them.	
Are there alarms for the computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.	

INTERNAL FIRE SUPPRESSION AND FIRE FIGHTING SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Alarms	
Does the entire asset/facility (or at least most of it) have a fire and/or smoke detection and alarm system? If yes, specify the type of system, how it is monitored, and the response procedure.	
(b) Fire Suppression	
Does the entire asset/facility (or at least most of it) have a fire suppression system such as an overhead sprinkler system? If yes, specify the medium (usually water) and whether it is of the flooded-pipe or pre-armed type.	
Does the water supply for the fire suppression system come from city water mains or an on-site system, such as wells, rivers, or reservoir?	
If the water supply for the fire suppression system comes from city water mains, specify whether there are separate city fire mains and if the pipe from the main to the asset/facility is separate from the domestic water supply.	
If the water supply for the fire suppression system comes from an on-site system, specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).	
(c) Fire Fighting	
Does the asset/facility have its own fire-fighting department? If yes, describe it in terms of adequacy to protect the asset/facility.	
Are city or community fire-fighting services available to the facility? If yes, indicate the type of service and the estimated response time.	
Does the water supply for the fire-fighting hydrants come from city water mains? If yes, specify the number of hydrants and indicate their coverage and accessibility.	
If the water supply for the fire fighting hydrants comes from an on-site system (such as wells, rivers, or reservoir), specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric). Also, specify the number of hydrants and indicate their coverage and accessibility.	
(d) Other Systems	
Is there special fire suppression equipment, such as Halon, Inergen, inert gases, or carbon dioxide in certain areas such as computer or telecommunications areas? If yes, indicate the types and adequacies of these special systems.	

INTERNAL SCADA SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Type of System	
Does the asset/facility make use of a substantial SCADA system (i.e., one that covers a large area or a large number of components and functions)? If yes, indicate what functions are monitored and/or controlled, the type of system, and the extent of the system.	
Is the SCADA system independent of the asset's/facility's primary electric power supply and distribution system?	
Is the SCADA system independent of the asset's/facility's telephone system?	
Is the SCADA system independent of the asset's/facility's microwave or radio communications system?	
Is the SCADA system independent of the asset's/facility's computers and servers?	
(b) Control Centers	
Where is the primary control center for the SCADA system located?	
Is there a backup control center? If yes, where is it located? Is it sufficiently remote from the primary control center to avoid common causes of failure such as fires, explosions, or other large threats?	
Are there backups to the SCADA computers and servers at the backup control center or at some other location? If yes, indicate the location of the backup computers and servers, whether they are completely redundant or cover only the most critical functions, and whether they are active "hot" standbys or have to be activated and initialized when needed.	
Note:*The following sets of questions on electric power sources and communications pathways apply to the control centers as well as the other components of the SCADA system.*	
(c) Electric Power Sources	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the SCADA system? If yes, indicate the types.	
If there is a special UPS, does it support all the functions of the SCADA system in terms of capacity? Specify for how long it can operate on battery power.	
If there is a special backup generator system, does it support all the functions of the SCADA system in terms of capacity?	
What is the fuel or fuels used by the special SCADA backup generator system? If stored on site, specify the quantity stored and how long it will last.	

If the SCADA backup generator fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	
(d) Communications Pathways	
Are there dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system? If yes, specify whether copper-wire or fiber-optic based.	
If there are dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system, is each one individually adequate to support the entire system? Specify any limitations.	
Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.	
Are the dedicated SCADA telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify type of protection.	
Are there dedicated multiple or redundant radio communications systems in place to support the SCADA system? If yes, indicate the types.	
If there are multiple radio communications systems, is each one individually adequate to support the entire SCADA system? If not, specify any limitations.	
Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the special SCADA radio communications systems? If yes, specify under what conditions and for how long.	
Do the special SCADA radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.	
Are the components of the special SCADA radio communications system located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security provided.	
(e) Remote Components	
Are there remote components to the special SCADA radio communications system (such as relay towers)? If yes, identify the components and there locations.	
Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.	
Are there environmental controls required for the remote components of the special SCADA radio communications system (such as heating, cooling)? If yes, describe them.	

Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.	
Is physical security provided for the remote components of the special SCADA radio communications system? If yes, specify the types of security and the level of protection provided.	
Are there alarms at the remote components of the special SCADA radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and to the response procedure.	
(f) Dedicated SCADA Computers and Servers	
Are there provisions within the asset's/ facility's primary electric power supply and distribution system to supply power for the special dedicated SCADA computers and servers? If yes, specify under what conditions and for how long.	
Do the special dedicated SCADA computers and servers have their own backup electric power supply, such as local UPSs? If yes, specify the types and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for the separate special SCADA computer and server areas?	
How long can the separate dedicated SCADA computers and servers operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated SCADA computer and server areas have their own independent environmental control system? If yes, specify the type.	
Are there any backup environmental controls explicitly for the dedicated SCADA computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.	
Is there special physical security provided for the separate SCADA computer and server areas? If yes, specify the type of security and the level of protection provided.	
Is there special fire suppression equipment in the separate dedicated SCADA computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.	
Are there special features or equipment in the separate SCADA computer and server areas to limit flooding or water intrusion? If yes, indicate the precautions taken.	
Are there alarms for the separate SCADA computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.	

INTERNAL DOMESTIC WATER SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Primary System	
Does the asset/facility have a domestic water system? If yes, specify the uses of the water (such as restrooms, locker rooms, kitchens, HVAC makeup water).	
Does the water supply for the domestic water system come from an external source (such as community, city, or regional water mains) or from an internal system (such as wells, river, or reservoir)? If internal, describe the system.	
(b) External Water Supply System	
What type of external water supply system provides the domestic water? Indicate whether it is public or private and its general size (such as community, city, or regional).	
Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.	
Are the on-site booster water pumps normally dependent upon the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site booster pumps at required levels? Also indicate the type of fuel or fuels used.	
If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last.	
If the fuel for the dedicated backup generator for the booster pumps is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	
(c) Internal Water Supply System	
Indicate the source of the water (such as wells, river, or reservoir), the adequacy of the supply's capacity, and whether it is gravity feed or requires active pumps (generally electric).	
Are the on-site domestic water system pumps independent of the asset's/facility's primary electric power supply and distribution system?	

Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site domestic water system pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site domestic water system pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site domestic water system pumps at the required levels? Also indicate the type of fuel or fuels used.	
If the fuel for the dedicated backup generator system for the on-site domestic water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(d) Backup System	
Is there an independent backup water source to the primary domestic supply system? If yes, specify the type of backup system (such as wells , river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).	
Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.	
If there is a special UPS, can it support the backup domestic water source pumps at the required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the backup domestic water source system pumps at the required levels? Also indicate the type of fuel or fuels used.	
If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	

INTERNAL INDUSTRIAL WATER/WASTEWATER SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Primary Water System	
Does the asset/facility have an industrial water system? If yes, specify the uses of the water (such as wash water, process water, generation of process steam, cooling).	
Does the water supply for the industrial water system come from an external source (such as community, city, or regional water mains) or from an internal system (such as wells, river, or reservoir)? If internal, describe the system.	
(b) External Water Supply System	
What type of external water supply system provides the industrial water? Indicate whether it is public or private and its general size (such as community, city, or regional).	
Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.	
Are the on-site booster water pumps for the industrial water system independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site booster pumps at required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(c) Internal Water Supply System	
Indicate the source of the water (such as wells, river, or reservoir), the adequacy of the supply's capacity, and whether it is gravity feed or requires active pumps (generally electric).	
Are the on-site industrial water system pumps independent of the asset's/facility's primary electric power supply and distribution system?	

Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial water system pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site industrial water system pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site industrial water system pumps at the required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the on-site industrial water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(d) Backup Water System	
Is there an independent backup water source to the primary industrial water supply system? If yes, specify the type of backup system (such as wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).	
Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.	
If there is a special UPS, can it support the backup industrial water source pumps at the required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the backup industrial water source system pumps at required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(e) Primary Industrial Wastewater System	
Does the asset/facility have an on-site industrial wastewater system? If yes, specify the types of wastewater that are processed and the processes used.	
Are the on-site industrial wastewater lift pumps independent of the asset's/facility's primary electric power supply and distribution system?	

Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial wastewater lift pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site industrial wastewater lift pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site industrial wastewater lift pumps at the required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the on-site industrial wastewater lift pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
f) Backup Wastewater System	
Is there an independent backup system that can be used to handle the industrial wastewater? If yes, specify the type of backup system (such as a redundant system, holding ponds, temporary discharge of unprocessed wastewater), describe the specific process, indicate the adequacy of the backup's capacity and any limitations on how long it can operate, and indicate if it is gravity feed or requires active lift pumps (generally electric).	
Are the independent backup lift pumps independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup wastewater lift pumps? If yes, specify them.	
If there is a special UPS, can it support the backup industrial wastewater system at the required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the backup industrial wastewater lift pumps at required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the backup wastewater lift pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	

INTERNAL PHYSICAL SECURITY SYSTEM

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Electric Power Sources	
Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the asset's/facility's primary electric power supply and distribution system the primary electric power source)?	
Are there multiple sources of electric power for the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the monitoring and alarm systems. Specify what electric power sources are in place.	
If there is a special UPS, can it support all the functions of the monitoring and alarm systems in terms of capacity? Specify for how long it can operate on battery power.	
If there is a special generator system, can it support all the functions of monitoring and alarm systems in terms of capacity? Also indicate the type of fuel or fuels used.	
If the fuel for the special security generator system is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(b) Communications Pathways	
Are the asset's/facility's monitoring and alarm systems normally dependent upon the asset's/facility's telephone system?	
Are there multiple independent telephone systems or dedicated switches and cables supporting the monitoring and alarm systems? This could consist of the asset's/facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber optic-cable based.	
Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.	

Are the dedicated monitoring and alarm systems telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify type of protection.	
Are the asset's/facility's monitoring and alarm systems normally dependent upon the asset's/facility's microwave or radio communications system?	
Are there multiple independent microwave or radio communications systems supporting the monitoring and alarm systems? This could consist of the asset's/facility's primary microwave or radio communications system and its backup or redundant systems; or combinations of multiple independent radios, antennae, and relay towers. Specify the type of radio systems used.	
Are there multiple sources of electric power for the microwave or radio communications systems dedicated to support the monitoring and alarm systems? This could consist of the asset's/facility's electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the special microwave or radio communications systems. If yes, specify the types and how long they can operate.	
Are the components of the special radio communications system dedicated to the monitoring and alarm systems that are located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.	
Are there remote components to the special radio communications system dedicated to the monitoring and alarm systems (such as relay towers)? If yes, identify the components and their locations.	
Are there backup sources of electric power for the remote components? If used, indicate the type of backup, the fuels used, and the expected length of operations.	
Are there environmental controls required for the remote components of the special monitoring and alarm radio communications system (such as heating, cooling)? If yes, describe them.	
Are there backup environmental controls for the remote components? If yes, indicate the type of backup, the fuel or fuels used, and the expected length of operations.	
(c) Computer Support	
Are the asset's/facility's monitoring and alarm systems normally dependent upon the facility's main computers and servers?	

Are there multiple independent computers supporting the monitoring and alarm systems? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric power for any computers dedicated to support the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the monitoring and alarm systems. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for the separate dedicated computers for the monitoring and alarm systems?	
How long can the separate dedicated computers of the monitoring and alarm systems operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers for the monitoring and alarm systems have their own independent environmental control system? If yes, specify the type.	
Are there backup environmental controls explicitly for any dedicated computers of the monitoring and alarm systems? If yes, indicate the type of backup and the expected maximum duration of operation.	

INTERNAL HUMAN RESOURCES SUPPORT

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Electric Power Sources	
Are the asset's/facility's human resources offices and functions normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the asset's/facility's primary electric power supply and distribution system the primary electric power source?)?	
Are there multiple sources of electric supply for the human resources offices and functions? This could consist of the facility's electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs, dedicated to support the human resources offices and functions? Specify what electric power sources are in place.	
If there is a special UPS, can it support all the human resources offices and functions? Specify for how long it can operate on battery power.	
If there is a special generator system, can it support all the human resources offices and functions? Also indicate the type of fuel or fuels used.	
If the fuel for the special generator system to support human resources is a petroleum fuel indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(b) Communications Pathways	
Are the asset's/facility's human resources offices and functions normally dependent upon the asset's/facility's telephone system?	
Are there multiple independent telephone systems or dedicated switches and cables supporting the human resources offices and functions? This could consist of the facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber optic-cable based.	
Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.	

Are the dedicated telephone switches and data-transfer switches that support the human resources offices and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.	
(c) Computer Support	
Are the asset's/facility's human resources offices and functions normally dependent upon the facility's main computers and servers?	
Are there multiple independent computers supporting the human resources offices and functions? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric power for any computers dedicated to support the human resources offices and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support human resources. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for any separate dedicated computers that support the human resources offices and functions?	
How long can the separate dedicated computers that support the human resources offices and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers that support the human resources offices and functions have their own independent environmental control system? If yes, specify the type.	
Are there backup environmental controls explicitly for any dedicated computers that support the human resources offices and functions? If yes, indicate the type of backup and the expected maximum duration of operation.	

INTERNAL FINANCIAL SYSTEM
(Including Monetary Transactions)

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Electric Power Sources	
Are the asset's/facility's financial systems and functions normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the facility's electric power supply and distribution system the primary electric power source?)?	
Are there multiple sources of electric power for the financial systems and functions? This could consist of the facility's electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions? Specify what electric power sources are in place.	
If there is a special UPS, can it support all the financial systems and functions? Specify for how long it can operate on battery power.	
If there is a special generator system, can it support all the financial systems and functions? Also indicate the type of fuel or fuels used.	
Is the fuel for the special security generator system a petroleum fuel? Specify the quantity stored and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
(b) Communications Pathways	
Are the asset's/facility's financial systems and functions normally dependent upon the asset's/facility's telephone system?	
Are there multiple independent telephone systems or dedicated switches and cables supporting the financial systems and functions? This could consist of the facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber-optic cable based.	
Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.	

Are the dedicated telephone switches and data-transfer switches that support the financial systems and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.	
(c) Computer Support	
Are the asset's/facility's financial systems and functions normally dependent upon the facility's main computers and servers ?	
Are there multiple independent computers supporting the financial systems and functions? This could consist of the facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric supply for any computers dedicated to support the financial systems and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for any separate dedicated computers that support the financial systems and functions?	
How long can the separate dedicated computers that support the financial systems and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers that support the financial systems and functions have their own independent environmental control system? If so, specify the type.	
Are there any backup environmental controls explicitly for the dedicated computers that support the financial systems and functions? If yes, indicate the type of backup and the expected maximum duration of operation.	

EXTERNAL ELECTRIC POWER INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Electric Power Sources	
How many substations feed the area of the asset/ facility and the asset/facility itself? That is, is the area supplied by multiple substations? If more than one, which ones have sufficient individual capac-ities to supply the critical needs of the asset/facility?	
How may distinct independent transmission lines supply the substations? Indicate if an individual substation is supplied by more than one transmission line and which substations are supplied by independent transmission lines.	
(b) Electric Power Pathways	
Are the power lines into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground.	
Do the power lines from these substations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.	
Are the paths of the power lines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.	
Are the paths of the power lines located in areas susceptible to natural or accidental damage (such as overhead lines near highways; power lines across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
(c) Electric Power Contracts	
What type of contract does the asset/facility have with the electric power distribution company or transmis sion companies? Specify the companies involved and whether there is a direct physical link (distribution or transmission power line) to each company.	
If there is an interruptible contract (even in part), what are the general conditions placed up interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has electric service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.	
(d) Historical Reliability	
Historically, how reliable has the commercial electric power been in the area? Quantify in terms of annual number of disruptions and their durations.	
Typically, when power outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify the duration of the outages.	
Have there ever been electric power outages of sufficient frequency and duration so as to affect the critical functions and activities of the asset/facility?	

EXTERNAL NATURAL GAS INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Sources of Natural Gas	
How many city gate stations supply the natural gas distribution system in the area of the asset/facility and the asset/facility itself? If more than one, which ones are critical to maintaining the distribution system?	
How may distinct independent transmission pipelines supply the city gate stations? Indicate if an individual gate station is supplied by more than one transmission pipeline and which stations are supplied by independent transmission pipelines.	
(b) Pathways of Natural Gas	
Do the distribution pipelines from the individual city gate stations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.	
Are the paths of the pipelines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.	
Are the paths of the pipelines located in areas susceptible to natural or accidental damage (such as across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
Is the local distribution system well integrated (i.e., can gas readily get from any part of the system to any other part of the system)?	
(c) Natural Gas Contracts	
Does the asset/facility have a firm delivery contract, an interruptible contract, or a mixed contract with the natural gas distribution company or the transmission companies? Specify the companies involved and whether there is a direct physical link (pipeline) to each company.	
If there is an interruptible contract (even in part), what are the general conditions placed up interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has natural gas service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.	

Does the asset/facility have storage or some other sort of special contracts with natural gas transmission or storage companies? If yes, briefly describe the effect on sustaining a continuous supply of natural gas to the asset/facility.	
In case of a prolonged disruption of natural gas supply, are contingency procedures in place to allow for the use of alternative fuels (such as on-site propane-air, liquefied petroleum gas, or petroleum fuels)? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility	
(d) Historical Reliability	
Historically, how reliable has the natural gas supply been in the area? Quantify by describing any unscheduled or unexpected disruptions. Were there any effects on the critical functions and activities of the asset/facility?	
If operating under an interruptible service agreement, has natural gas service ever been curtailed? If yes, how often, for how long, and were there any effects on the critical functions and activities of the asset/facility?	

EXTERNAL PETROLEUM FUELS INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Uses of Petroleum Fuels	
Are petroleum fuels used in normal operations at the asset/facility? If yes, specify the types and uses.	
Are petroleum fuels used during contingency or emergency operations such as for backup equipment or repairs? If yes, specify the types of fuels and their uses.	
(b) Reception Facilities	
How are the various petroleum fuels normally delivered to the asset/facility? Indicate the delivery mode and normal frequency of shipments for each fuel type.	
Under maximum use-rate conditions, are there sufficient reception facilities (truck racks, rail sidings, surge tank capacity, barge moorings) to keep up with maximum contingency or emergency demand)? If no, explain where the expected shortfalls would be and their impacts.	
Are the petroleum fuel delivery pathways co-located with the rights-of-way of other infrastructures or located in areas susceptible to natural or accidental damage (across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
Are contingency procedures in place to allow for alternative modes or routes of delivery? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility.	
(c) Supply Contracts	
Are contracts in place for the supply of petroleum fuels? Specify the contractors, the types of contracts, the modes of transport (pipeline, rail car, tank truck), and the frequency of normal shipments.	
Are arrangements for emergency deliveries of petroleum fuels in place? Indicate the basic terms of the contracts in terms of the maximum time to delivery and the minimum and maximum quantity per delivery. Also, indicate if these terms are such that there may be effects on the critical functions and activities of the asset/facility.	

EXTERNAL TELECOMMUNICATIONS INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Telecommunications Carriers	
Are there multiple telecommunications carriers used by the asset/facility (possibly commercial, contracted, or organization-owned)? List them, specify the service they provide or the type of information carried (such as analog telephone voice and FAX, digital telephone voice, internet connections, dedicated data transfer), and the type of media used (copper cable, fiber-optic cable, microwave, satellite).	
(b) Pathways of Telecommunications Cables	
Are the telecommunications cables into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground.	
Do the telecommunications cables follow independent pathways into the area of the asset/facility and into the asset/facility itself? If not, indicate how independent they are (some common corridors, intersect at one or more points).	
Are the paths of the telecommunications cables co-located with the rights-of-way of other infrastructures? If yes, describe the extent of the co-location and indicate the other infrastructures.	
Are the paths of the telecommunications cables located in areas susceptible to natural or accidental damage (such as overhead cables near highways; cables across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
Do the various telecommunications carriers and cable pathways use separate independent end offices (EO), access tandems (AT), points of presence (POP), and network access points (NAP) to reach the communications transmission backbones? Briefly describe the extent of this independence.	
(c) Historical Reliability	
Historically, has the public switched network (PSN) telephone system in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.	
Typically, when telephone outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activates at the asset/facility.	

Historically, have the internet and dedicated data transfer systems in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.	
Typically, when internet or data transfer connectivity outages or disruptions occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activates at the asset/facility.	
(d) Backup Communications Systems	
Are there redundant or backup telephone systems in place if the primary system is disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.	
Are there redundant or backup internet and dedicated data transfer systems in place if the primary systems are disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.	

EXTERNAL WATER AND WASTEWATER INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Water Supply Reliability	
Historically, has the city water supply in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the supply pressure or flow rate.	
Typically, when disruptions in the city water supply occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.	
(b) Wastewater System Reliability	
Historically, has the public wastewater system in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the capacity of the system.	
Typically, when disruptions in the public wastewater system occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.	
Are there any contingency plans or procedures in place to handle domestic wastewater from the asset/facility if the public system is temporarily unable to accept the waste? If yes, describe them and mention any limitations on quantity of wastewater and duration of outage that might affect the ability of the asset/facility to carry out critical functions or activities.	

EXTERNAL ROAD TRANSPORTATION INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Road Access	
Are there multiple roadways into the area of the asset/facility from the major highways and interstates? Describe the route or routes and indicate any load or throughput limitations with respect to the needs of the asset/facility.	
Are there any choke points or potential hazard areas along these roadways such as tunnels, bridges, dams, low-lying fog areas, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.	
(b) Road Access Control	
Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by road without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vehicles, and the size or quantity of material that could approach the asset/facility by road.	
Are there uncontrolled parking lots or open areas for parking near the facility where vehicles could park without drawing significant attention? If yes, indicate the number of vehicles and the size or types of vehicles that would begin to be noticed.	

EXTERNAL RAIL TRANSPORTATION INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Rail Access	
Are there multiple rail routes into the area of the asset/facility from the nearby rail yards or switchyards? Describe the route or routes and indicate any load or throughput limitations with respect to the needs of the asset/facility.	
Are there any choke points or potential hazard areas along these rail rights-of-way such as tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, rail traffic closures have occurred somewhat regularly.	
Is there sufficient rail siding space at or near the asset/facility to accommodate rail cars if the number of incoming cars exceeds normal expectations or if outgoing cars are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities of the asset/facility would be affected.	
(b) Rail Access Control	
Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by rail without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people and rail cars that could approach the asset/facility by rail.	
Are there railroad tracks or sidings near the asset/facility where rail cars could be positioned without drawing significant attention? If yes, indicate the number and the types of rail cars that would begin to be noticed.	

EXTERNAL AIR TRANSPORTATION INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Airports and Air Routes	
Are there multiple airports in the area of the site of sufficient size and with sufficient service to support the critical functions and activities at the asset/facility? Enumerate the airports and indicate any limitations.	
Are there any regular air routes that pass over or near the asset/facility that could present a danger to the asset/facility if there were some sort of an air disaster? Record any concerns.	

EXTERNAL WATER TRANSPORTATION INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Waterway Access	
Are there multiple water routes to the ports, harbors, or landings used by the asset/facility from the open ocean or major waterway? Describe the route or routes and indicate any load, draft, beam, or throughput limitations with respect the needs of the organization.	
Are there any choke points or potential hazard areas along these waterways such as bridges, draw or lift bridges, locks and dams, low-lying fog areas, or landslide areas? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.	
Is there sufficient mooring, wharf, or dock space at the ports, harbors, or landings used by the asset/facility to accommodate ships or barges if the number of incoming vessels exceeds normal expectations or if outgoing barges are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities at the asset/facility would be affected.	
(b) Waterway Access Control	
Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by water without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vessels, and the size or quantity of material that could approach the asset/facility by water.	
Are there uncontrolled docks or mooring areas near the asset/facility or the ports, harbors, or landings used by the asset/facility where vessels could moor without drawing significant attention? If yes, indicate the number of vessels and the size or types of vessels that would begin to be noticed.	

EXTERNAL PIPELINE TRANSPORTATION INFRASTRUCTURE

Date: _____ Facility: _____

This checklist applies to:

Entire Facility

Critical Asset _____

	COMMENTS
(a) Pipeline Access	
What materials feedstocks or products (such as crude oil, intermediate petroleum products, refined petroleum products, or liquefied petroleum gas—do not include water, wastewater, or natural gas unless there are special circumstances related to these items) are supplied to or shipped from the asset/facility by way of pipeline transportation?	
Are there multiple pipelines and pipeline routes into the area of the asset/facility from major interstate transportation pipelines? If yes, indicate which pipelines or combinations of pipelines have sufficient capacity to serve the asset/facility.	
List the pipeline owners/operators, indicate the types of service provided (dedicated or scheduled shipments), describe the route or routes, and indicate any capacity limitations with respect the needs of the asset/facility.	
Are there any bottlenecks or potential hazard areas along these pipelines or pipeline routes such as interconnects, terminals, tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, outages or delays have occurred somewhat regularly.	
(b) Pipeline Access Control	
Could intruders or others determined to bring down the asset/facility gain access to the pipeline near the asset/facility or elsewhere along the pipeline route? Describe the protective measures that are in place and indicate any pipeline segments or facilities (such as pump stations, surge tanks) of concern.	

OPSEC TABLES

HUMAN RESOURCES SECURITY PROCEDURES

Date: _____ Facility: _____

	COMMENTS
(a) Responsibilities	
What organization(s) is responsible for dealing with security-related personnel issues?	
(b) Background Checks	
Are background checks done on employees? If yes, for which employees?	
Is the background check done for selected (sensitive) positions? If yes, what are the criteria for identifying sensitive positions?	
How extensive are the background checks? Do they vary with the sensitivity of the position?	
(c) Insider Threats	
Are there current conditions in the company that might create a threat from insiders (e.g., low morale, lay-offs, labor disputes)?	
Are there security procedures for handling disgruntled or at-risk employees? If yes, describe.	
What are the security procedures for handling terminated employees? How many have been terminated in the last year? Have there been any security incidents related to a terminated employee?	
(d) Disciplinary Procedures	
What are the policies and procedures for incidents of security concern?	
What are the policies and procedures for other disciplinary actions?	
(e) Security Training	
Is there a company Security Awareness training program that includes initial and periodic security training? Does it include sections on security contacts, critical assets, threats, sensitive information that needs to be protected, reporting suspicious activities, and employee responsibility?	
(f) Travel	
Are employee travel records (e.g., authorizations, vouchers, trip reports) protected? If yes, describe how.	

FACILITY ENGINEERING

Date: _____ Facility: _____

This section covers security issues related to the engineering information related to the facility. Included are the facility design, configuration, and layout; utility service systems; building floor plans; etc.

	COMMENTS
(a) Responsibilities	
What organization(s) is responsible for facility engineering?	
(b) Facility Engineering Information	
What facility engineering information (e.g., engineering drawings, site maps, utility service lines, floor plans, entry paths into the facility, etc.) is available?	
What organization(s) has control of this information?	
What other internal organizations are allowed access to this information?	
What external organizations (e.g., fire department, environmental agency) have been given access to this information?	
Is any of the facility engineering information publicly available?	
Can sensitive information be gleaned from commercial overhead imaging (e.g., aerial photography, commercial satellite images)? If yes, describe.	
How is this information protected?	
Is this information on the computer system or network?	
How is the information disposed of when no longer needed?	
(c) Public Access to Facility	
Are tours allowed of any or all of the facility? If yes, describe what portions of the facility are open and who is allowed to tour.	
Is any portion of the facility open to the public or special interest groups? If yes, describe.	
Are periodic meetings held where outsiders are allowed inside the facility? If yes, describe.	
Are there procedures for security escorting of visitors? If yes, describe.	

FACILITY OPERATIONS

Date: _____ Facility: _____

	COMMENTS
(a) Responsibilities	
What organization(s) is responsible for facility operations?	
(b) Facility Operations Control	
Is the operation of the facility controlled from a central point (or several central points)? Describe.	
Is there an automated process control system, energy management system, SCADA system? If yes, describe. If yes, is it isolated or is there remote access possibility?	
Is facility operations control and information on computer systems? If yes, how is it protected? What other internal organizations have access to operations control capability and information?	
Can sensitive operations information be gathered through the telecommunications system (e.g., microwave, cell phones, RF, pagers, voicemail, teleconferencing)?	
Is access to the control point(s) limited to operations personnel? If no, who else has access (e.g., maintenance, janitors, vendors, etc.) and how is that access controlled?	
(c) Facility Construction, Repair, and Maintenance	
Is construction, repair and maintenance at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.	
Is cleaning and building maintenance (e.g., janitorial service) at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.	

ADMINISTRATIVE SUPPORT ORGANIZATIONS

Date: _____ Facility: _____

	COMMENTS
(a) Procurement	Purchasing and procurement activities including: Generating Need (e.g., requisition or RFP), Selecting Supplier, Documenting the Purchase, Providing Delivery of Item or Service, Payment.
What organization(s) is responsible for reviewing procurement activities from a security perspective?	
What is the process used to review RFPs, contracts, and other procurement documents for security-related information?	
How is the procurement information protected before release? Include documents, files, copiers, facsimiles, computer files?	
Is security-sensitive information uniquely marked, both on paper and electronically? If yes, describe how.	
How is security-sensitive procurement information destroyed?	
How are company credit cards controlled? Who is authorized to have one? How is security-related information from credit card use identified and protected?	
(b) Legal	
What organization(s) is responsible for reviewing legal department activities from a security perspective?	
How are legal documents (e.g., patents, environmental impact statements, safety reports, Securities and Exchange Commission filings, Federal Energy Regulatory Commission filings, etc.) reviewed for security implications?	
How are these documents protected?	
(c) Budget and Finance	
What organization(s) is responsible for reviewing budget and finance activities from a security perspective?	
How are budget and finance documents reviewed for security implications?	
How are these documents protected?	
(d) Marketing	
What organization(s) is responsible for reviewing marketing activities from a security perspective?	
How are marketing materials reviewed for security implications?	
How are these documents protected?	
(e) Internal Information	
Are there policies and procedures for handling "Internal Use Documents" (e.g., memos, notes, newsletters, etc.)? If yes, describe.	
How are these documents protected?	
How are these documents destroyed when no longer needed?	

TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Date: _____ Facility: _____

This checklist covers telecommunications, information technologies, and cyber security. Note that this part of the operations security survey must coordinated with the portions of the interdependencies survey that address the telecommunications and computer equipment.

	COMMENTS
(a) Telecommunications	
What telecommunications equipment is in regular use: __ Telephone __ Cell phones __ Voicemail __ Fax __ Audio/video conferencing __ Radio __ Microwave __ Other_____	
Does particular equipment carry sensitive traffic? If yes, describe.	
Are particular nodes susceptible to intercept? If yes, describe.	
Is particular equipment restricted to selected users? If yes, describe.	
Are internal telephone lines routed to external switches? If yes, describe.	
Can any telecommunications equipment be operated in reverse as eavesdropping equipment? If yes, describe.	
Are there connections to external radio nets, including paging nets? If yes, describe.	
Is voicemail protected by passwords? Have users changed the vendor-supplied passwords? Is there a master password?	
How are fax machines protected? How is the stored information protected?	
Is encryption used on any telecommunications circuits?	
(b) Information Technology	
Is there a corporate security architecture for the computer network? If yes, describe. Does it include intrusion detection, firewalls, compartmentalization? If yes, describe.	
What computer information is available to outsiders?	
How are computer applications developed (internal, external)? How is software and hardware maintenance performed?	
What are the policies and procedures for passwords?	
Is there dial-up access for operations, maintenance, or other reasons? If yes, describe.	
Are there embedded computer systems in other systems (e.g., HVAC equipment, numerically controlled machines, etc.)? If yes, how are they protected?	
Is there a computer incident response team? If yes, describe.	
Are exercises (“War Dialing”) conducted to locate unauthorized modems? If yes, describe.	
Is encryption used for internal files and/or information transmission? If yes, describe.	
Have system administrators been trained to recognize “social engineering attacks” designed to obtain passwords and other security information? If yes, describe.	
Is e-mail monitored? If yes, describe.	

PUBLICLY RELEASED INFORMATION

Date: _____ Facility: _____

This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.

	COMMENTS
(a) Responsibilities	
What organization(s) is responsible for reviewing information (from a security perspective) that is to be released to the public?	
(b) General Procedures	
What is the process used to review information before release?	
How is the information protected before release? Include documents, files, copiers, facsimiles, computer files.	
(c) Report Release	
Who is responsible for reviewing reports released by the company?	
Who generates the reports?	
What type of information is included?	
What is the distribution and ultimate disposition of company-released reports?	
(d) Press Contacts	
Are specific people designated to interact with the press?	
How are they trained (including training on security issues)? Who trains them?	
(e) Briefing and Presentations	
Are briefings and presentations to be given by company employees reviewed for security issues? If yes, describe how.	
(f) Public Testimony	
Is public testimony that is to be given by company employees reviewed for security issues? If yes, describe how.	
(g) Internet Information	
Is there a policy in place to review information posted on the company Internet site for security issues? If yes, describe.	
Who reviews information before it is posted on the Website?	
Is the Website reviewed and monitored regularly for security-related information? If so, describe how.	

TRASH AND WASTE HANDLING

Date: _____ Facility: _____

This checklist covers the handling of trash and waste that may have security implications (e.g., documents records, discarded equipment, etc.)

	COMMENTS
(a) Responsibilities	
What organization is responsible for security of trash and waste?	
Are there established policies for trash and waste handling? If yes, describe.	
(b) Trash Handling	
Where is trash accumulated?	
Is the trash accessible to outsiders?	
Who collects the trash?	
Where is the trash taken?	
(c) Paper Waste Handling	
Where is paper waste accumulated?	
Are shredders available and used? If yes, describe.	
Is the paper waste accessible to outsiders?	
Who collects the paper waste?	
Where is the paper waste taken? Is it sent for recycling?	
Is there on-site destruction of paper waste? If yes, describe how it is protected until destroyed.	
(d) Salvage Material Handling	
Does salvage material (e.g., serviceable equipment no longer needed, surplus equipment) potentially contain sensitive information?	
Is salvage material inspected prior to release? If yes, by whom? Describe procedures.	
(e) Dumpster Control	
Are dumpsters (for trash, paper waste, salvage material) that are accessible to the public monitored to prevent “dumpster diving”? If yes, describe how.	
Are publicly accessible dumpsters sampled for sensitive information?	

Appendix C1—Refinery SVA Example

The application of the SVA Methodology to a fictitious refinery is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the refinery company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A—SVA Methodology Flow Diagram

Form 1—Critical Assets/Criticality form

Form 2—Threats Worksheet
Form 3—Attractiveness/Target Ranking Form

Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Form 1—Critical Assets/Criticality form

Determine the major assets of the refinery including processes, control rooms, gates and access control points, marine terminals, terminus points for export and import pipelines, utilities, and supporting infrastructure. All entry points should be evaluated as an asset in order to focus the analysis on the need for perimeter security and access control. The team lists all relevant assets on Form 1 in Column 1. Similar facilities with similar geographic locations, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set. In Column 2, document the design basis of the asset and the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen. In the Column 3 rank the estimated overall severity of the loss of the asset. Use the five-level Severity Ranking scale for severity or develop an equivalent as required for the particular facility.

Form 2—Threats Worksheet

Document the threats against the facility on Form 2. Include consideration in Column 1 of general types of adversaries that will be considered (usually terrorists, disgruntled employee or contractor, or extreme activist as an example, but more specific or other groups can be considered as required); Column 2 is the source of the attack (EXT—External to the facility, INT—Internal to the facility); Column 3 documents the threat specific to the facility being evaluated; Column 4 documents the specific or general threat of that type of adversary against this or similar assets worldwide; Column 5 documents the potential actions that the adversary could take; Column 6 documents the assumed capabilities, weapons, tactics, and sophistication of the adversary; Column 7 documents their level of motivation; Column 8 provides for an overall ranking assessment per the Threat Ranking scale or equivalent.

Form 3—Attractiveness/Target Ranking Form

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum of the different adversary's interests to a common assete may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

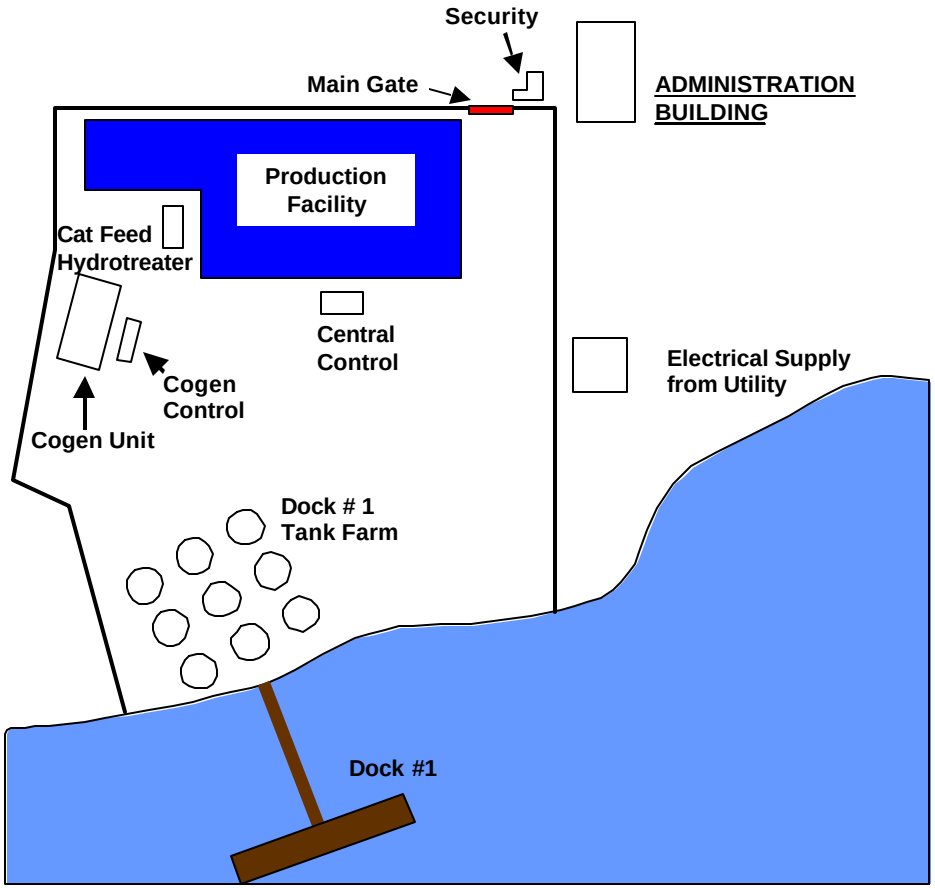
Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Column 1 is the Security Event Type (see Step 3.3—generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

Responsibilities

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the refinery owner/operator. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

Fictitious Refinery Example



Form 1: Critical Assets/Criticality Form

Facility Name: Fictitious Refinery

Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1. Administration building	Administrative offices including management offices and large number of employees, HR Manager; ordinary office building hazards; personnel exposure to approximately 100 persons; possible loss of personnel and/or critical documents in storage (business sensitive information).	3
2. Central Control Room	Critical security communications and monitoring; Cat, Coker 1, Alkylation, Treating Plant; Crude Units; loss of control function and long time to repair if damaged.	5
3. Cogen Unit and Control Room	Critical steam production and supplemental electrical power generation.	4
4. Dock 1	Loss of logistics for feedstock and products; environmental release; fire and explosion; possible to shutdown channel; coker feed, #2 fuel oil, benzene, toluene, molten sulfur in storage; Coker feed is most critical feedstock.	5
5. Dock 1 Tank Farm—storage in atmospheric tanks north of Dock 1 (crude inT-800; T-802; T-803,T-805; ballast/slop oil tank T-804; lube oils in T-240 to T-244)	Flammable and combustible liquids fire and explosion hazard; possible spill to ship channel; critical to operation of marine terminal.	4
6. Cat Feed Hydrotreater Unit	Significant fire and explosion hazard onsite; possible public impacts from explosion; significant business interruption.	5
7. Electrical supply from Utility to Refinery	Utility supplied; Cat Feed HT, H2 plant, and Units 29 – 35; backup supply from other substations.	3
8. Units 29-35 cooling tower/chlorine containers	Important to operation of units 29 – 35; chlorine toxic hazards may have public impact if damaged.	4

Form 2: Threats Worksheet

Facility Name: Fictitious Refinery

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Assumed Adversary Capability	Adversary Motivation	Threat Ranking
1. Terrorist	EXT	No specific group or threat to the refinery	- General industry terrorist threats only - HSAS Yellow as of the time of the SVA	- Use explosives or small arms to destroy target - May be interested in theft of products of value to terrorist organizations for secondary attack	- Use of improvised explosive device possibly involving a vehicle is most likely scenario - Assume trained, with good information and significant resources to plan and execute attack	Assume highly motivated to cause maximum damage to critical infrastructure and casualties	4
2. Disgruntled employee or contractor	INT	Employees and contractors	- Company facilities have had telephone bomb threats - No actual damage but threats have been made. - Assume general industry experience with insider sabotage is credible	- Might cause intentional overfill of tank or damage to equipment leading to release; might cause product contamination; possible for explosion - Possible for workplace violence - Potential for theft	- Specialized insider knowledge and training - Unrestricted access to entire facility - Not likely to use weapons if sabotage but may use small arms if workplace violence	Potential for disgruntled employee due to disciplinary action; other workplace violence reasons; possibly in collusion with outside terrorist group in extreme case	3
3. Activist	EXT	Citizens for Green Environment has expressed interest	Multiple demonstrations have occurred at the plant	Possibly interested in causing public embarrassment; temporary shutdown of plant; long range goal of elimination of toxic substance in use.	- Highly organized; well funded to cause staged attack of multiple facility operations simultaneously (dock, rail, gate)	Highly politically charged and motivated	4

Form 3: Attractiveness/Target Ranking Form

Facility Name: Fictitious Refinery

Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
1. Administration building	Administrative offices including management offices and large number of employees, HR Manager; approximately 100 persons; possible loss of personnel and/or critical documents in storage (process and business sensitive information)	3	Management offices and large number of employees and computer systems	2	Management offices and large number of employees; HR Manager	3	Possibly interested in seeking out management for protest but not accessible directly and Business Services building is more accessible	2	TR3
2. Central Control Room	Critical security communications and monitoring; Crude 1, Alkylation, Treating Plant	4	Provides access to control multiple units at the same time	4	Maybe recognizable target; insider information on process control and access; high concentration of processes under single control and large numbers of operators in plant	3	Not easily accessible; does not provide opportunity for media attention and requires trespassing	2	TR4
3. Dock 1	All crude receipts and product transfers occur over Dock 1; hazard of flammable liquids spill and fire and oil spill on water. Possible for disruption to entire refinery and adjacent facilities if waterway is blocked.	5	Immediately accessible; recognizable and importance well understood; critical to refinery operation; long lead time for repair; complicating to adjacent facilities	4	Accessibility; importance well understood; critical to refinery operation; long lead time for repair	4	Could be easily accessible by watercraft; provides opportunity for media attention; activist activity against dock in past.	3	TR4

Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures

Facility Name: Fictitious Refinery

Critical Assets: 20. Dock 1

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Countermeasures	Vulnerability	Vulnerability Ranking	L	R	New Countermeasures
1.1. Loss of containment	Terrorist	**I/E**	Attack on vessel or dock facility by way of an improvised explosive device	Damage to barge and dock facilities; loss of logistics for feedstock and products; major environmental release; fire and explosion; possible to shutdown channel	S5	1.1. USCG boat patrols of the channel and port 1.2 Roving guardforce	1.1. Lack of access control from water, 1.2 Low lighting 1.3No intrusion detection	5	L4	High	Consider improving lighting, access control, monitoring by CCTV, and administrative controls per requirements of Enclosure 2 of NVIC 11-02.

Appendix C2—Fictitious Pipeline Example

The application of the SVA Methodology to a fictitious petroleum liquids pipeline system is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the pipeline company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of the pipeline system from both the general viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the system level. The benefit of evaluating specific assets is that individual risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

For example, all facilities will maintain a minimum level of security with general countermeasures such as the pipeline shutdown and control strategies and administrative security controls. Certain assets will justify a more specific level of security based on their value and expected level of interest to adversaries.

The SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire pipeline system, the assets that comprise the pipeline system, the critical functions of the pipeline, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are "critical" to the business operation. Criticality may be defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance and continuity of the system. For example, a pumping station or a specific branch along the pipeline system may be a critical part of the operation of the pipeline system due to inability to operate without it or, if attacked, it has the greatest impact. As such it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. As shown in Figure A, all assets receive at least a general security review. This is accomplished by the basic SVA team's consideration as an asset to begin with, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix F.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A— SVA Methodology Flow Diagram

Form 1—Critical Assets/Criticality form

Form 2—Threats Worksheet
Form 3—Attractiveness/Target Ranking Form

Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Form 1—Critical Assets/Criticality form

Determine the major assets of the pipeline system including control rooms, gates and access control points, marine terminals, communications networks, terminus points for export and import pipelines, utilities, and supporting infrastructure. All entry points to critical facilities should be evaluated as an asset in order to focus the analysis on the need for perimeter security and access control. The team lists all relevant assets on Form 1 in Column 1. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set. In Column 2, document the design basis of the asset and the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen. In the Column 3 rank the estimated overall severity of the loss of the asset. Use the five-level Severity Ranking scale for severity or develop an equivalent as required for the particular facility.

Form 2—Threats Worksheet

Document the threats against the pipeline system or a critical facility on Form 2. Include consideration in Column 1 of general types of adversaries that will be considered (usually terrorists, disgruntled employee or contractor, or extreme activist as an example, but more specific or other groups can be considered as required); Column 2 is the source of the attack (EXT—External to the pipeline/facility, INT—Internal to the pipeline/facility); Column 3 documents the threat specific to the pipeline/facility being evaluated; Column 4 documents the specific or general threat of that type of adversary against this or similar assets worldwide; Column 5 documents the potential actions that the adversary could take; Column 6 documents the assumed capabilities, weapons, tactics, and sophistication of the adversary; Column 7 documents their level of motivation; Column 8 provides for an overall ranking assessment per the Threat Ranking scale or equivalent.

Form 3—Attractiveness/Target Ranking Form

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

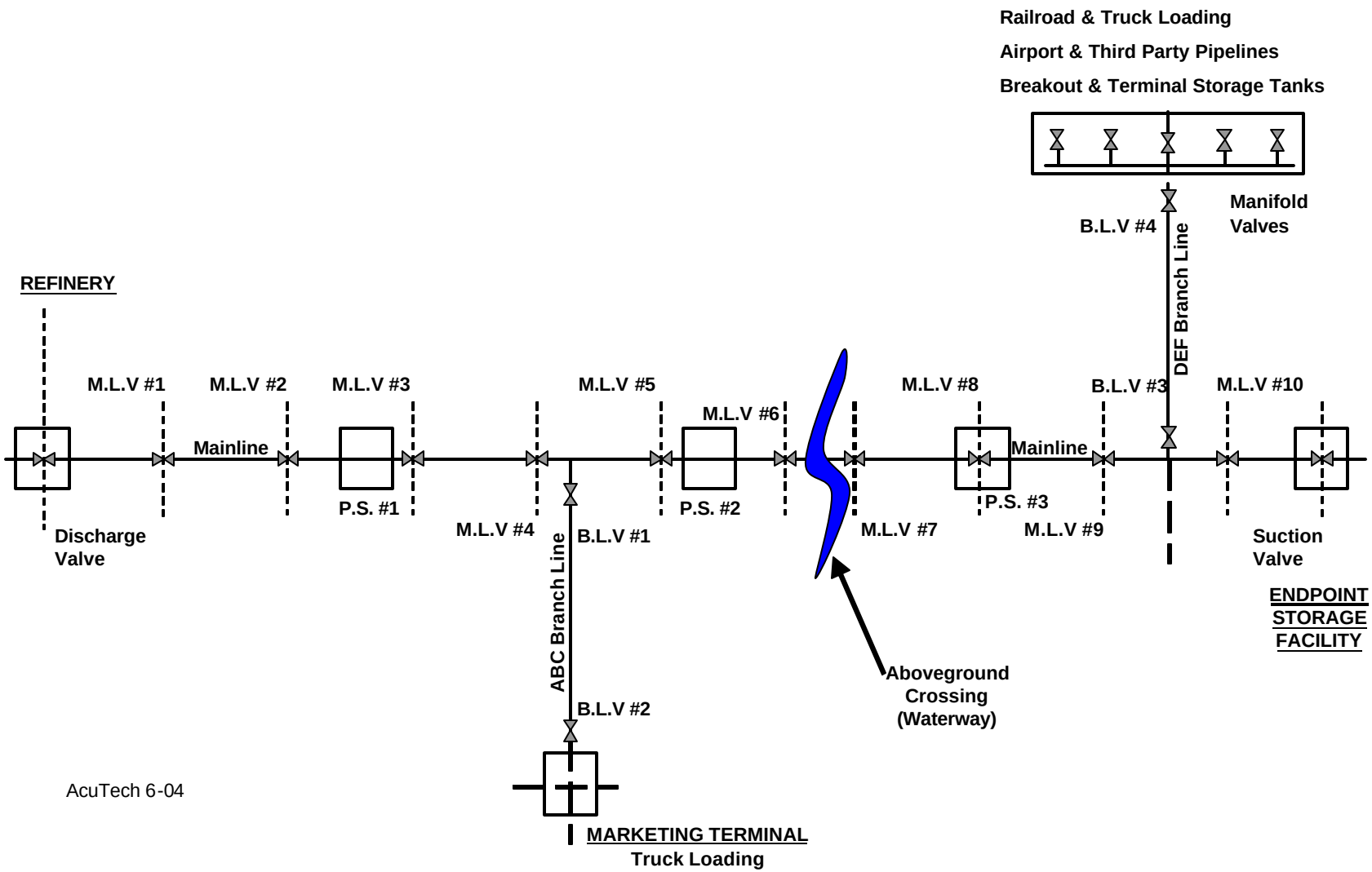
Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Column 1 is the Security Event Type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New /Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

Responsibilities

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the pipeline owner/operator. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

Fictitious Pipeline Example



Form 1: Critical Assets/Criticality Form

Facility Name: 1. Fictitious Pipeline Company

Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1. Main Line, 24-inch Liquids Pipeline System—1000 miles, provides 500,000 b/d. Finished products; Gasoline, Jet Fuel and home heating oil. 35 main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas.	Main line serves large metropolitan areas. Several million retail customers plus 5 major international airports, and two large military installations. Includes a major above ground river crossing, which provides drinking water to large urban community.	5
2. ABC Branch—10 miles, 8 inch branch line serving mixed products to marketing terminal serving a rural population.	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available.	1
3. DEF Branch and inter-modal terminal—Branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines and direct connect to military, commercial airports and power plant.	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers.	4
4. Endpoint storage facility—Major tank farm for large metropolitan area, airport and other party pipeline connection.	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.	2
5. River Span Block Valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair.	5
6. River Span Pipeline (Above Ground)	Above ground river span (see 1 above). Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean up costs. No alternate mode to market. Significant service interruption.	5
7. Inter-modal Terminal	Large inter-modal products terminal with rail, truck and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to 2 major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact. Limited public safety and employee impact.	4

Form 2: Threats Worksheet

Facility Name: 1. Fictitious Pipeline Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Threat Ranking
International terrorists	**I/E/C**	No site-specific history of international terrorism.	There have been numerous international terrorist acts against petroleum pipelines in the world to date. Most notably in South America and Middle East. U.S. Homeland Security Advisory System is rated orange presently. According to recent FBI repots, Al Qaeda continues to show interest in the energy sector and large scale operations that have significant impacts to public safety, the national economy, and national symbol of American might and wealth.	Use of stealth or force to cause damage and/or release of hydrocarbons. Possible theft or contamination of product possible but not likely. Degradation of assets and interruption of service biggest concern. Possible environmental release into public water supply and public safety are concerns. Damage to equipment and time to repair are also issues.	High level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	4
Domestic Terrorist or Activist	**I/E/C**	History at the main-line system of multiple bomb threats over the pas t 2 years. All concluded were fakes.	No confirmed domestic acts of terrorism on the pipeline infrastructure.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations.	Low level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small arms and explosives.	Adversary intent is to cause economic harm through service interruption. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, possibly without personal sacrifice.	3

Form 2: Threats Worksheet

Facility Name: 1. Fictitious Pipeline Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Threat Ranking
Disgruntled Employee or Contractor	**INT**	No evidence of sabotage has been discovered in the past.	Minimal acts of sabotage or workplace violence.	Sabotage to equipment including SCADA causing possible release of hazardous materials, contamination of products, environmental impact, or major equipment damage and business interruption. Possible for nuisance threats, particularly from contract workers with intent to disrupt operations.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to keys, computer passwords, gate access codes, communication equipment, records, vehicles, proximity cards for access cards, company process control system.	Nuisance adversary is intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	4

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Pipeline Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
1. Main Line, 24-inch Liquids Pipeline System—1000 miles, provides 500,000 b/d. Finished products; Gasoline, Jet Fuel and home heating oil. 35 main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas.	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available.	5	Easy access due to length of pipeline and location in a rural area with several above ground - unmanned pumping stations. Minimal disruptions to only a rural customer base no impact to military and minimal potential environmental impact.	1	Some insider insight helpful but not necessary.	2	Limited interest.	2	TR 2
2. ABC Branch—10 miles, 8 inch branch line serving mixed products to marketing terminal serving a rural population.	Main line serves large metropolitan areas. Several million retail customers plus 5 major international airports, and two large military installations. Includes a major above ground river crossing, which provides drinking water to large urban community.	1	Major disruption to residential, air travel and military. Public safety and drinking water contamination. Easy access.	2	Some insider insight helpful but not necessary.	2	Public Image impact due to press/media interest.	3	TR 3

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Pipeline Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
3. DEF Branch and inter-modal terminal—Branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines and direct connect to military, commercial airports and power plant.	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers.	4	Major disruption to air travel, power supply and military. Easy access.	3	Some insider insight helpful but not necessary.	2	Public Image impact due to press/media interest.	3	TR 3
4. Endpoint storage facility—Major tank farm for large metropolitan area, airport and other party pipeline connection.	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.	2	Hardened facility. Access difficult but impact significant.	3	Insider information very helpful both to gain access and operational.	2	Nuisance issue with trespassing. Public image impact. Operational knowledge needed.	2	TR 3
5. River span block valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair.	5	Public safety and drinking water contamination. Perhaps included with attack on asset--River Span (above ground).	2	Some insider insight helpful but not necessary. Difficult access within minimal success.	1	Limited interest.	2	TR 2

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Pipeline Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
6. River Span Pipeline (Above Ground)	Above ground river span (see 1 above). Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean up costs. No alternate mode to market. Significant service interruption.	5	Public safety and drinking water contamination. Easy access.	3	No insider knowledge needed for breach/access.	1	Public Image impact due to press/media interest.	3	TR 3
7. Inter-modal Terminal	Large inter-modal products terminal with rail, truck and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to 2 major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact. Limited public safety and employee impact.	4	Hardened facility. Access difficult but impact significant.	3	Insider information very helpful both to gain access and operational.	2	Nuisance issue with trespassing. Public image impact. Operational knowledge needed.	2	TR 3

Form 4—Scenario Based Vulnerability

Facility Name: 1. Fictitious Pipeline Company

Critical Assets: 6. River Span Pipeline (Above Ground)

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Safeguards/ Countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Destruction of span, release of product and loss of containment.	Terrorist	**I/E/C**	Destruction of river span by bombing.	Damage of river span; release of product into river; contamination of public drinking water supply; loss of service to downstream facilities for an extended period.	S5	1.1. Fencing around cable platform.	1. There are some protective measures; river span remote; easy access - above grade.	4	L3	High	1. Consider additional hardening to prevent access to river span.
						1.2. Air patrol and ground observation.					2. *Evaluate additional intrusion detectors feasible at this site.
						1.3. Manually operated block valve.					3. *Evaluate if CCTV is feasible.
						1.4. Monitoring pipeline conditions and flow ctrl.					4. Consider additional surveillance of this area.

**Note: Additional countermeasures should be based on threat and criticality of the equipment / system under evaluation. Due to remote locations, electric power may not be available or feasible to implement electronic security measures.*

Form 4—Scenario Based Vulnerability

Facility Name: 1. Fictitious Pipeline Company

Critical Assets: 7. Inter-modal Terminal

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Safeguards/ Countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Destruction of inter-modal terminal manifold piping.	Terrorist	**I/E/C**	Destruction of piping by bombing.	Inability to receive or pump product and possible onsite fatalities.	S4	1.1. Fencing, lighting, access control, CCTV, manned 24/7, security procedures in place.	1. There are multiple protective measures but at least one weakness to gain access.	2	L3	Med	5. Consider improved access control, 24/7 security guards at higher threat levels. 6. Consider additional countermeasures to achieve “protection in Depth” such as random vehicle inspections, background checks.

Appendix C3—Fictitious Truck Transportation SVA Example

The application of the SVA Methodology to a fictitious products distribution system by truck is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the owner of the trucking company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

The example is of a fictitious hydrocarbon tank truck transportation system, which includes the tank truck, inventory of flammable liquids and the route specific variables such as the type of road, population centers and environmental receptors, and any stops. It is assumed that the shipper and receiver sites will have a separate SVAs. This example is intended to provide some insight on how one might conduct a security vulnerability analysis (SVA) using this methodology on the fictitious truck transportation system. This example is not intended to be all inclusive of every situation or every item that one may consider when conducting an SVA on a tank truck system. It is recognized that not all tank truck systems are the same. Factors such as route length, type of cargo, geographic location and many other factors play a significant role to determine the criticality of the transportation system thereby defining the type and level of analysis that may be appropriate for a particular situation.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A—SVA Methodology Flow Diagram

Form 1—Critical Assets/Criticality form

Form 2—Threats Worksheet
Form 3—Attractiveness/Target Ranking Form

Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Form 1—Critical Assets/Criticality form

First determine the major assets of the truck transportation system including function, major customers, routes, check points, terminals, utilities, and supporting infrastructure. Next, critical facilities or functions of the transportation system are identified. For all critical facilities, identify critical assets within those functions or within those facilities. All entry points should be evaluated as an asset in order to focus the analysis on the need for perimeter security and access control. The team lists all relevant assets on Form 1 in Column 1. Similar facilities with similar geographic locations, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set. In Column 2, document the design basis of the asset and the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen. In the Column 3 rank the estimated overall severity of the loss of the asset. Use the five-level Severity Ranking scale for severity or develop an equivalent as required for the particular facility.

Form 2—Threats Worksheet

Document the threats against the transportation system/facility on Form 2. Include consideration in Column 1 of general types of adversaries that will be considered (usually terrorists, disgruntled employee or contractor, or extreme activist as an example, but more specific or other groups can be considered as required); Column 2 is the source of the attack (EXT—External to the transportation system/facility, INT—Internal to the transportation system/facility); Column 3 documents the threat specific to the transportation system/facility being evaluated; Column 4 documents the specific or general threat of that type of adversary against this or similar assets worldwide; Column 5 documents the potential actions that the adversary could take; Column 6 documents the assumed capabilities, weapons, tactics, and sophistication of the adversary; Column 7 documents their level of motivation; Column 8 provides for an overall ranking assessment per the Threat Ranking scale or equivalent.

Form 3—Attractiveness/Target Ranking Form

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

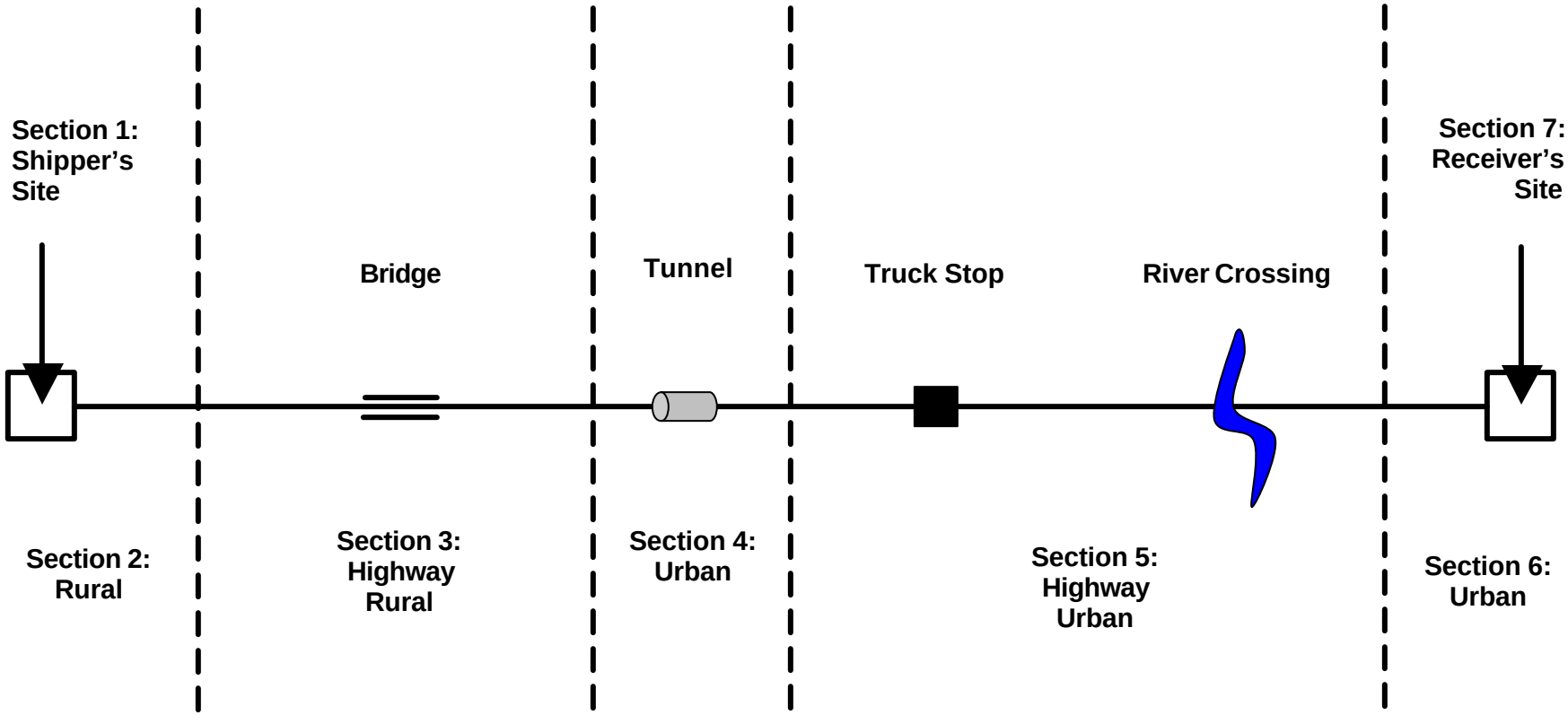
Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Column 1 is the Security Event Type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New /Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

Responsibilities

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the Shipper. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with owner/operators of adjacent facilities, Receivers, and infrastructure providers as required for risk communication and completeness.

SVA Methodology
Fictitious Truck Transportation Example



Form 1: Critical Assets/Criticality Form

Facility Name: 1. Fictitious Trucking Company

Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1. Tank Truck containing petroleum products and loading rack operations	Shipper loads 50 tank trucks per day of products and dispatches them to both local receivers and to within nearby neighboring states. Route evaluated is the longest distance transported to a receiver's site. Potential for flammable liquids to be attacked directly to damage the loading rack and operations, to be attacked while en route to cause collateral damage, or to be hijacked and used as a weapon against other targets.	4
2. Rural section of road leading from the Shipper's Site to HWY 100 – 15 miles, traversing primarily rural areas.	Single entrance/exit to supplier's site, but incident involving tank truck on this section of route would result in limited impacts due to low population density.	2
3. HWY 100 (50 miles) traversing primarily through rural areas.	Long stretch across rural section of route.	3
4. Bridge along HWY 100.	Potential to block/damage bridge if tank truck attacked on the bridge.	3
5. Downtown section of route along State Route 5 (15 miles), traversing through high population density area.	Highest population density along route, but shortest segment.	3
6. Tunnel along State Route 5 leading into downtown.	Potential to block/damage tunnel preventing entrance/exit to the city and possible for multiple fatalities/injuries from occupants in other vehicles in tunnel.	4
7. HWY 200 (100 miles) traversing through primarily urban areas.	Longest stretch along the route with a high population density along the segment, potential to not only impact vehicle occupants on road but also surrounding population impacts.	4
8. Truck Stop along HWY 200.	Potential for theft/access to unmanned vehicle.	4
9. River Span along HWY 200.	Potential for environmental impact if product released into river.	3
10. Urban route off HWY 200 to Receiver's site - 10 miles.	Single entrance/exit to receiver's site, with potential for fatalities/injuries due to high population density surrounding the site.	3

Form 2: Threats Worksheet

Facility Name: 1. Fictitious Trucking Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
International terrorists	I/E/C	1.1. No site-specific history of intentional acts against ACME.	According to information bulletins from DHS there have been suspicious activities involving bulk facilities including surveillance and following trucks. International terrorists have targeted trucks for highjackings and direct attacks.	Use of force to cause damage to vehicles while in transit or at loading/offloading facilities. This could cause a release of hydrocarbons and resulting fire and explosion with possible fatalities and injuries and degradation of transportation assets and environmental release. Terrorists may be interested in 1) weaponization of a tank truck to use fuels as a improvised, field-ready weapon at another location 2) directly damage the truck and cause collateral damage and disruption to the supply chain 3) "Trojan Horse" attack where the truck is used to introduce a weapon into a facility.	Assume a high level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	Credible threat. Include in analysis. An attempt to cause a violent attack on the truck would be consistent with both the tactics and goals of domestic terrorists.	3

Form 2: Threats Worksheet

Facility Name: 1. Fictitious Trucking Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
Domestic Terrorist or Activist	I/E/C	2.1. History of bomb threats at ACME Trucking. All concluded were fakes--no bomb or activist found. ACME has had activist protest at the main gate within the past 2 years.	No confirmed domestic acts of terrorism against fuels trucking operations.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations, similar to international terrorist objectives but most-likely of a less severe nature. Possible actions would include highjackings, theft, vandalism, and arson.	Assume medium level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small improvised explosive devices.	Adversary intent is to cause economic harm through service interruption or to emphasize a political cause. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, but more-likely without personal sacrifice.	Credible threat. Included in analysis. An attempt to cause damage or disruption to operation is likely in the future.	3

Form 2: Threats Worksheet

Facility Name: 1. Fictitious Trucking Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
Disgruntled Employee or Contractor	INT	3.1. No evidence of sabotage has been discovered in the past. Have been several safety systems compromised and incidences of theft.	There have been acts of sabotage, theft and arson to the petroleum trucking operations in the past.	Sabotage to vehicles, including safety systems, arson, and theft of product.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to vehicles, facilities, gate access codes, communication equipment, records, and proximity cards for access cards.	Disgruntled employee is most-likely intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	Credible threat. Include in analysis.	2

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Trucking Company

Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
1. Tank truck containing 10,000 gallons of hydrocarbons.	Shipper dispatches 50 trucks per day of gasoline to both local receivers and to within nearby neighboring states. Route evaluated is the longest distance transported to a receiver's site.	3	Potential for release resulting in large fire, potential fatalities and closure/damage to major transportation route.	3	Insider information necessary to gain access to vehicle.	1	Public image impact due to press/media interest.	2	TR3
2. Rural section of road leading from the Shipper's Site to HWY 100 – 15 miles, traversing primarily rural areas.	Single entrance/exit to supplier's site, but incident involving tank truck on this section of route would result in limited impacts due to low population density.	1	Short section of route and limited number of potential impacts.	1	No additional attraction.	1	No additional attraction.	1	TR1
3. HWY 100 (50 miles) traversing primarily through rural areas.	Long stretch across rural section of route.	2	Minimal attraction due to limited impact potential, but length of route provides access to vehicle.	2	No additional attraction.	1	No additional attraction.	1	TR2

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Trucking Company

Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
4. Bridge along HWY 100.	Potential to block/damage bridge if tank truck attacked on the bridge.	3	Potential to cause major disruption to US Highway as well as result in potential fatalities and injuries.	3	No additional attraction.	1	Potential to block bridge.	2	TR3
5. Downtown section of route along State Route 5 (15 miles), traversing through high population density area.	Highest population density along route, but shortest segment.	3	High population density and potential to harm a large number of people.	3	No additional attraction.	1	No additional attraction.	1	TR3
6. Tunnel along State Route 5 leading into downtown.	Potential to block/damage tunnel preventing entrance/exit to the city and possible for multiple fatalities/injuries from occupants in other vehicles in tunnel.	3	High population impact potential as well as potential to disrupt local economy by blocking tunnel.	3	No additional attraction.	1	Potential to block tunnel.	2	TR3
7. HWY 200 (100 miles) traversing through primarily urban areas.	Longest stretch along the route with a high population density along the segment, potential to not only impact vehicle occupants on road but also surrounding population.	3	Long section of route provides access to truck highly populated area.	3	No additional attraction.	1	No additional attraction.	1	TR3
8. Truck Stop along HWY 200.	Potential for theft/access to unmanned vehicle.	3	Potential to gain access to truck--theft.	2	No additional attraction.	1	No additional attraction.	1	TR2
9. River Span along HWY 200.	Potential for environmental impact if product released into river.	2	Material not likely to cause sustained environmental impact.	1	No additional attraction.	1	No additional attraction.	1	TR1
10. Urban route off HWY 200 to Receiver's site – 10 miles.	Single entrance/exit to receiver's site, with potential for fatalities/injuries due to high population density surrounding the site.	2	Limited access due to shortness of route, but high population density makes section attractive.	2	No additional attraction.	1	No additional attraction.	1	TR2

Form 4—Scenario Based Vulnerability

Facility Name: 1. Fictitious Trucking Company

Critical Assets: 1. Tank Truck containing 10,000 gallons of hydrocarbons

Scenario Worksheet Form											
Security Event Type	Threat Category	Threat Type	Undesired Act	Consequences	S	Existing Safeguards/ Countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Truck is attacked enroute resulting in a release of hydrocarbons.	Terrorist	**I/E/C**	Release and ignition of hydrocarbons on a major roadway.	Potential fatalities and injuries from resulting fire. Possible closure of a major transportation route.	S4	1.1. Experienced/ Licensed Drivers-- background checks before employment.	1. Longest route exposes the truck many hours per shipment; provides the opportunity for surveillance and unexpected attack; route also passes along several areas of high population density, including bridge and tunnel.	4	L3	High	1. Consider developing company system to alert drivers to DHS/FBI alerts.
						1.2. Identification of driver's checked at both the shipper and receiver's sites.					2. Consider developing a system to cont act local law enforcement at DHS “red” levels for information prior to traveling.
						1.3. Drivers trained in HAZMAT.					3. Consider providing security awareness and emergency action training to drivers.
						1.4. Truck is in constant radio contact while enroute.					
1.2. Truck is highjacked enroute.	Terrorist	**I/E/C**	Loss of truck and product.	Potential for injury/fatality to driver in an attack by force. Loss of truck and product, but unlikely to be used in subsequent attack.	S4	2.1. Truck is in constant radio contact while enroute.	1. Long stretches of rural areas along route provide opportunity for surveillance and attack; truck is left unattended while at the truck stop.	3	L2	Med	4. Consider adding GPS tracking system to truck so that they can be tracked/located if stolen.
						2.2. Single scheduled truck stop along route.					5. Consider additional radio checks at elevated security levels.
						2.3. Truck is normally locked when driver is at the truck stop.					
						2.4. Truck has electronic disengagement systems.					

Appendix C4—Fictitious Rail Transportation SVA Example

The application of the SVA Methodology to a fictitious petroleum liquids pipeline system is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the shipper company and considers the various interfaces with customers, suppliers and en-route interfaces. However, the security of the customer and supplier facilities and the en-route interfaces is the responsibility of the owners of those facilities, as well as the general route risk assessment issues. An example may include the switchyard security plan. It is the responsibility of the switchyard operator to ensure the security of the switchyard.

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of the rail transportation system from both the general viewpoint and specific asset viewpoint. Consideration at the general overall route level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the route level. The benefit of evaluating specific assets is that individual interface risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

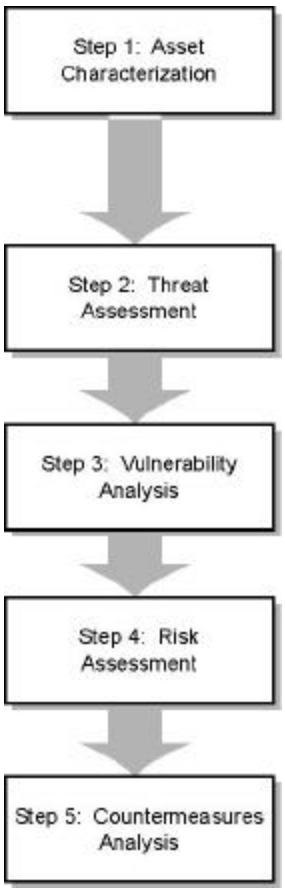
The SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire rail transportation route that applies to the route that the shipper's products take through the value chain from production facility to various customers and end users. The SVA will analyze the critical assets that comprise the transportation system, the critical functions of the system, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are "critical" to the business operation. Criticality may be defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance and continuity of the system. For example, a rail loading station or a specific branch along the route may be a critical part of the operation of the system due to inability to operate without it or, if attacked, it has the greatest impact. As such it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. As shown in Figure A, all assets receive at least a general security review. This is accomplished by the basic SVA team's consideration as an asset to begin with, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix F.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A—SVA Methodology Flow Diagram



Form 1—Critical Assets/Criticality form

Form 2—Threats Worksheet
Form 3—Attractiveness/Target Ranking Form

Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Form 1—Critical Assets/Criticality Form

Determine the major assets of the rail transportation system including loading facilities, switching yards, specific routes, control rooms, gates and access control points, marine terminals, bridges, tunnels, utilities, supporting infrastructure, and other considerations. All entry points to a facility should be evaluated as an asset in order to focus the analysis on the need for perimeter security and access control. The team lists all relevant assets on Form 1 in Column 1. Similar facilities with similar geographic locations, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set. In Column 2, document the design basis of the asset and the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen. In the Column 3 rank the estimated overall severity of the loss of the asset. Use the five-level Severity Ranking scale for severity or develop an equivalent as required for the particular facility or transportation system. Conduct the study on the overall general route, followed by more detailed evaluation of critical facilities.

Form 2—Threats Worksheet

Document the threats against the facilities or transportation system on Form 2. Include consideration in Column 1 of general types of adversaries that will be considered (usually terrorists, disgruntled employee or contractor, or extreme activist as an example, but more specific or other groups can be considered as required); Column 2 is the source of the attack (EXT—External to a facility or rail system, INT—Internal to a facility or rail system); Column 3 documents the threat specific to the facility or rail system being evaluated; Column 4 documents the specific or general threat of that type of adversary against this or similar assets and operations worldwide; Column 5 documents the potential actions that the adversary could take; Column 6 documents the assumed capabilities, weapons, tactics, and sophistication of the adversary; Column 7 documents their level of motivation; Column 8 provides for an overall ranking assessment per the Threat Ranking scale or equivalent.

Form 3—Attractiveness/Target Ranking Form

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset or operation is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

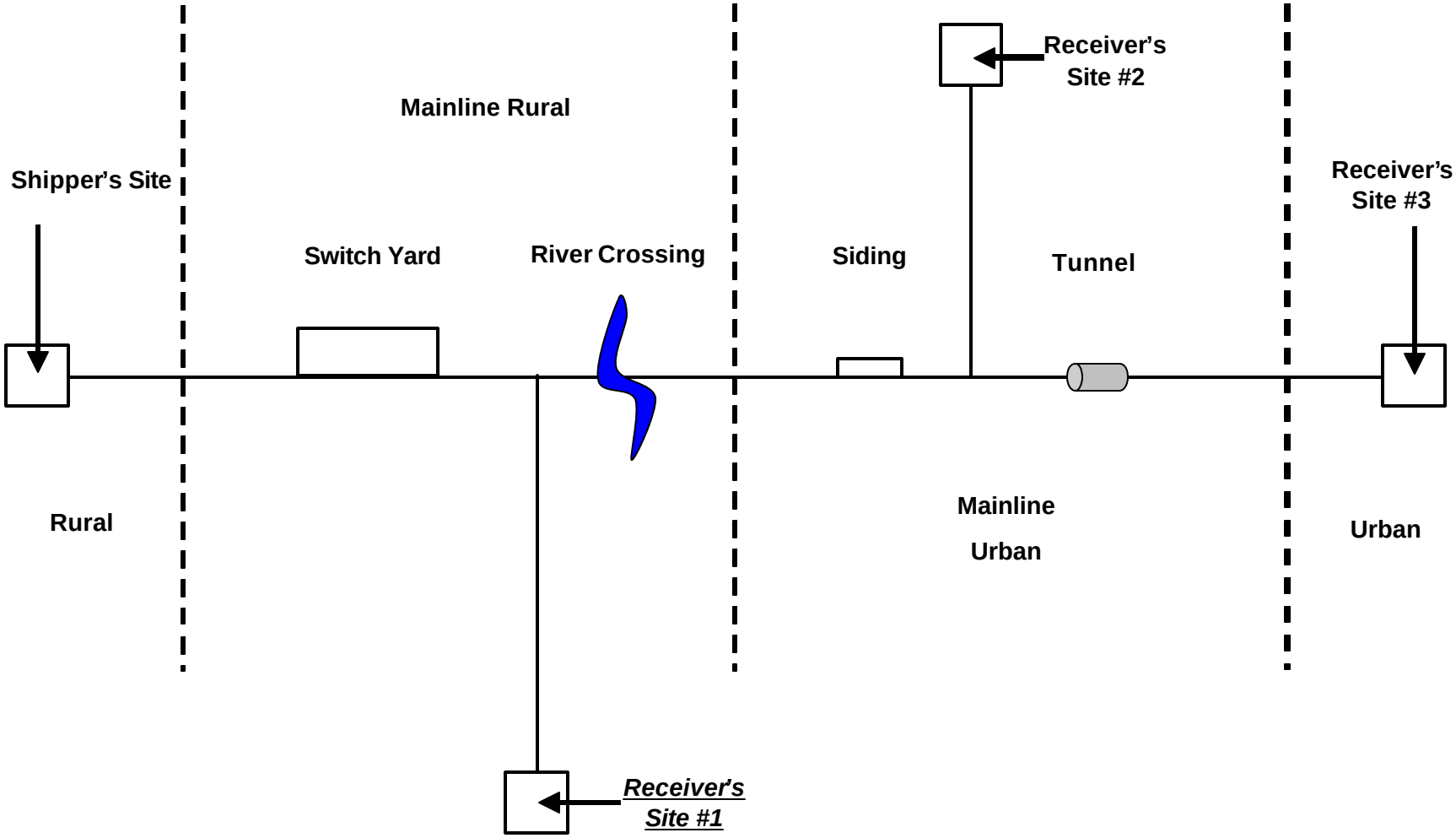
Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form

Column 1 is the Security Event Type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New /Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

Responsibilities

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the Shipper. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with railroad owner/operators, owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

API/NPRA SVA Methodology
Rail Transportation Example



AcuTech 5-04

Form 1: Critical Assets/Criticality Form

Facility Name: 1. Fictitious Rail Company

Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1. 25 railcars of petroleum products.	Two trains comprised solely of 25 petroleum products railcars are shipped daily from the shipper's terminal. After leaving the terminal the tankcars are divided into three separate trains at the switchyard and sent to three final receiver's sites. Site #1 - 25 railcars per day. Site #2 - 10 railcars per day. Site #3 - 15 railcars. En route from the switch yard to Site #1 is on a mainline track along a mostly rural area. En route to Site #2 and #3 crosses a river and have access to a siding as needed. The route to Site #2 branches off on an urban mainline, while the route to Site #3 continues through a tunnel before reaching its final destination. Potential hazard for this route is the potential to release one or more railcars resulting in a large environmental impact and or fire and subsequent fatalities and injuries if ignited.	4
2. Rural section of track to switch yard - 25 miles from shipper's site.	Single rail entrance/exit to supplier's site; incident involving railcar on this section of the route would result in limited fatalities/injuries due to low population density, but large fire could damage rail line.	3
3. Mainline section of track in rural area - 200 miles. Including rail spur to Receiver Site #1.	Long stretch across rural section of route.	3
4. Switch Yard	Switch point to individual trains to receiver's sites. Potential to damage site, other railcars and various products if petroleum products released and ignited.	4
5. River crossing	Potential for environmental impact if product released into river.	3
6. Mainline section of track in urban area - 300 miles. Including rail spurs to Site #2 and Site #3.	Long stretch across urban section on route to Site #2 and Site #3.	3
7. Siding in Urban Area (see 6)	Potential for theft/access to unmanned railcars.	4
8. Tunnel in Urban Area (see 6)	Potential to block/damage tunnel.	4

Form 2: Threats Worksheet

Facility Name: 1. ACME Rail Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
International terrorists	**I/E/C**	1.1. No site-specific history of intentional acts against ACME.	Bombings in Madrid have recently indicated the vulnerability of the rail transportation infrastructure.	Terrorists may be interested in 1) weaponization of a train to use fuels as a improvised, field-ready weapon at another location 2) directly damage the railcar(s) and cause collateral damage and disruption to the supply chain 3) "Trojan Horse" attack where the railcars are used to introduce a weapon into a facility.	Assume a high level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	Credible threat. Include in analysis. An attempt to cause a violent attack on the railcar/train would be consistent with both the tactics and goals of domestic terrorists.	3
Domestic Terrorist or Activist	**I/E/C**	2.1. History of bomb threats at ACME. No actual bombs found or activist groups claiming responsibility. ACME has had activist protest at the corporate headquarters within the past 5 years.	No confirmed domestic acts of terrorism against fuels rail operations.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations, similar to international terrorist objectives but most-likely of a less severe nature. Possible actions would include vandalism, blockage of track and arson.	Assume medium level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small improvised explosive devices.	Adversary intent is to cause economic harm through service interruption or to emphasize a political cause. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, but more-likely without personal sacrifice.	Credible threat. Included in analysis. An attempt to cause damage or disruption to operation is likely in the future.	3

Form 2: Threats Worksheet

Facility Name: 1. ACME Rail Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
Disgruntled Employee or Contractor	**INT**	3.1. No evidence of sabotage has been discovered in the past.	There have been acts of sabotage, theft and arson to the petroleum railcar operations in the past.	Sabotage to railcars including safety systems, and arson.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to railcars/train, facilities, gate access codes, communication equipment, records, and proximity cards for access cards.	Disgruntled employee is most-likely intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	Credible threat. Include in analysis.	4

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Rail Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
1. 25 railcars of petroleum products.	Two trains comprised of 25 petroleum products railcars are shipped daily from the shipper's terminal. After leaving the terminal the tankcars are divided into three separate trains at the switch yard and sent to three final receiver's sites. Site #1 - 25 railcars per day. Site #2 - 10 railcars per day. Site #3 - 15 railcars. Potential to release one or more railcars resulting in a large environmental impact and or fire and subsequent fatalities and injuries if ignited.	3	Potential for release resulting in large fire, potential fatalities and closure/damage to major transportation route.	3	Insider information necessary to gain access to vehicle.	1	Public image impact due to press/media interest.	2	TR 3
2. Rural section of track to switch yard - 25 miles from shipper's site.	Single rail entrance/exit to supplier's site; incident involving railcar on this section of the route would result in limited fatalities/injuries due to low population density, but large fire could damage rail line.	1	Short section of route and limited number of potential impacts.	1	No additional attraction.	1	No additional attraction.	1	TR 1
3. Mainline section of track in rural area - 200 miles. Including rail spur to Receiver Site #1.	Long stretch across rural section of route.	2	Minimal attraction due to limited impact potential, but length of route provides access to vehicle.	2	No additional attraction.	1	No additional attraction.	1	TR 2

Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Rail Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
4. Switch Yard	Switch point to individual trains to receiver's sites. Potential to damage site, other railcars and various products if petroleum products released and ignited.	2	Potential to cause major disruption to rail transportation systems.	3	No additional attraction.	1	Potential to block bridge.	2	TR 3
5. River crossing	Potential for environmental impact if product released into river.	2	Potential contamination of drinking water supply and major disruption to rail transportation system.	3	No additional attraction.	1	No additional attraction.	1	TR 3
6. Mainline section of track in urban area – 300 miles. Including rail spurs to Site #2 and Site #3.	Long stretch across urban section on route to Site #2 and Site #3.	3	High population density and potential to harm a large number of people. Ability to disrupt Sites #2/3	4	Ability to disrupt Sites #2/3	4	Ability to disrupt Sites #2/3	2	TR 4
7. Siding in Urban Area (see 6)	Potential for theft/access to unmanned railcars.	3	Siding provides access to unmanned railcars in populated area.	3	No additional attraction.	1	No additional attraction.	1	TR 3
8. Tunnel in Urban Area (see 6)	Potential to block/damage tunnel.	3	Potential to cause major disruption to rail transportation system.	2	No additional attraction.	1	No additional attraction.	1	TR 2

Form 4—Scenario Based Vulnerability

Facility Name: 1. Fictitious Rail Company

Critical Assets: 1. 25 railcars of petroleum products.

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Safeguards/ Countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Train is attacked en route with a bomb resulting in a release of petroleum products.	Terrorist	**I/E/C**	Release and ignition of petroleum products on a major roadway.	Possible closure/damage to major transport ion rail line and potential fatalities and injuries from resulting fire.	S4	1.1. Major Class I Railroad used to carry materials along the entire route to all receivers' sites. 1.2. Security Plan at both the shipper and receiver's site. 1.3. Train is in constant radio contact while en route.	1. Railcars are exposed many hours per shipment; provides the opportunity for surveillance and unexpected attack; route also passes along several areas of high population density and includes both bridge and tunnel.	4	L3	Med	1. Meet with rail company and develop security plan. Discuss access control and staging of cars at elevated threat levels. 2. Consider providing security awareness and emergency action training to rail personnel. 3. Review security procedures/plan at the switch yard; revise plan as necessary to address any security concerns
1.2. Bomb is attached to railcar while in switchyard or while on siding.	Terrorist	**I/E/C**	Bomb is brought onto receiver's site.	Explosion/fire on the rail spurs of at the receiver's site resulting in fatalities/injuries and potential damage to spur and receivers process equipment.	S4	2.1. Security Plan at both the shipper and receiver's site.	1. Railcars are exposed and vulnerable to placement of hidden bomb on railcar while in yard and while on spur.	5	L5	High	4. Meet with switchyard operator to review security issues. 5. Review security procedure at receiver's site for accepting and screening railcars for delivery. 6. Consider adding lighting and CCTV around siding to prevent access to stopped train, while en route.

References

"Chemical Accident Prevention Provisions" (part 68 of Title 40 of the *Code of Federal Regulations (CFR)*).

Chemical Facility Vulnerability Assessment Methodology, NIJ Special Report, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July, 2002.

Counterterrorism and Contingency Planning Guide. Special publication from Security Management magazine and American Society for Industrial Security, 2001.

Guidance Document for Implementing 40 *CFR* Part 68, USEPA, 1998.

Guidelines for Chemical Process Quantitative Risk Analysis, Second Ed., Center for Chemical Process Safety, American Institute of Chemical Engineers, 2000.

Guidelines for Consequence Analysis of Chemical Releases, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1999.

Guidelines for Technical Management of Chemical Process Safety, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1998.

Guidelines for Technical Planning for On-Site Emergencies, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.

Inherently Safer Chemical Processes – A Life Cycle Approach, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.

Layers of Protection Analysis, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2001.

"Site Security Guidelines for the U.S. Chemical Industry", American Chemistry Council, October, 2001.

Bowers, Dan M., "Security Fundamentals for the Safety Engineer", *Professional Safety*, American Society of Safety Engineers, December, 2001, pgs. 31-33.

Dalton, Dennis. *Security Management: Business Strategies for Success*. (Newton, MA: Butterworth-Heinemann Publishing, 1995).

Fischer, Robert J. and Green, Gion. *Introduction to Security*, 6th ed. (Boston: Butterworth-Heinemann, 1998).

Ragan, Patrick T., et al., "Chemical Plant Safety", *Chemical Engineering Progress*, February, 2002 pgs. 62-68.

Roper, C.A. *Physical Security and the Inspection Process* (Boston: Butterworth-Heinemann, 1997).

Roper, C.A. *Risk Management for Security Professionals* (Boston: Butterworth-Heinemann, 1999).

Walsh, Timothy J., and Richard J. Healy, eds. *Protection of Assets Manual* (Santa Monica, CA: Merritt Co.). Four-volume loose-leaf reference manual, updated monthly.

Additional copies are available through Global Engineering Documents at (800) 854-7179 or (303) 397-7956

Information about API Publications, Programs and Services is available on the World Wide Web at http://www.api.org

American Petroleum Institute

1220 L Street, Northwest
Washington, D.C. 20005-4070
202-682-8000

Product No: OSVA02