Note: The Appendices will not appear in the Code of Federal Regulations.

APPENDIX A

The Department believes that "risk" in the context of terrorism is a function of three variables: consequence (or criticality), vulnerability (or the likelihood that an attack will succeed if launched), and threat (or the likelihood that an attack would be launched in the first place). The Department also believes that "consequence" is the initial qualifying factor – that is, if a thing is not critical, then there will not be a significant level of risk associated with it. Accordingly, the Department intends to employ a consequence-only "Top-screen."

I. Purpose of the Top-screen Tool

The Top-screen is a basic questionnaire that facilities will be required to complete. It will provide the Department with information to make a preliminary determination as to the level of risk associated with any given facility. The Department will use it to screen facilities in order to eliminate as many as is appropriate from further activity under the regulation, and to prioritize those facilities that are, on preliminary assessment, "high risk." The Department will make the Top-screen available as an on-line tool.

II. Categories of Top-screen users

There will be two categories of Top-screen users: providers and submitters. A provider is a qualified individual familiar with the facility in question. This person will complete the screening tool. A submitter is an officer of the corporation (or equivalent) responsible for the facility in question. The submitter will send the completed Top-screen(s) to DHS, and in so doing, will attest to the accuracy of the information provided.

The provider and the submitter may be the same person should a facility owner/operator so choose. The provider will therefore have the option of "submitting" the completed Top-screen to DHS or forwarding it to the provider within his or her own organization.

DHS is considering the imposition of a requirement whereby the submitter must satisfy all of the following requirements: be an officer of the corporation, be a citizen of the United States, and be domiciled in the United States. The Department requests comment on this proposed requirement.

III. Top-screen Questions

The first segment of the Top-screen will focus on gathering identifying information from the facility, such as its name, address, identification numbers, corporate affiliation, and geo-location. During this segment, DHS will obtain essential contact information and will learn of the exact location of facilities.

The first segment of the Top-screen will also seek to gather information on criticality issues. It will ask questions directed at identifying criticality related to the:

- Potential loss of life (and life-changing injuries) on or near the facility;
- Potential loss of the capability to execute a critical mission, not only in defense, but also in governance and in the provision of essential services and utilities.

The second segment of the Top-screen will ask a series of exclusionary questions. For example, DHS will ask whether a facility is a public water system or a water treatment works facility, covered under MTSA, owned or operated by the Department of Defense or the Department of Energy, and/or licensed by the Nuclear Regulatory Commission. By asking these questions, DHS will be able to quickly "screen out" those facilities that are excluded by law from this regulation, yet will still be able to account for those facilities and to know why they are excluded from the regulation.

To address risk to human life, the third segment of the Top-screen will focus on identifying which chemicals are present at facilities. As part of the Top-screen tool, DHS will provide a list of chemicals and threshold quantities (TQ) for each listed chemical. A provider would be able to select (possibly through the use of a pull-down menu) those chemicals that are present (at any time or in the course of a year, depending on the chemical) in quantities equal to or above the stated TQ. Where the facility does not contain any such chemicals, the facility will be presumptively screened out of coverage from the regulation.

This segment will be broken down into several "pages," each of which addresses the security issues associated with specific chemicals and the TQs of those chemicals. In most (but not all) cases, these security issues will parallel the Department of Transportation's classes of hazards.

To address human health and safety consequences, the tool would ask the facility the following types of questions:

- Whether a toxic release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 200,000 persons, and if so, whether the distance in such a scenario might exceed 25 miles;
- Whether a flammable release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 1,000 persons;
- Whether the facility manufactures or stores explosive materials in sufficient quantities to result in an offsite residential exposed population;
- Whether the facility has any specified chemical weapon or chemical weapon precursors;

To address economic impacts, the tool would ask the facility the following types of questions:

- Whether the facility produces products of national economic importance or whose loss could negatively impact multiple economic sectors;
- Whether an attack on the facility could cause collateral physical damage to key transportation assets;

To address mission impacts the tool would ask questions, such as whether the facility:

- Has chemical(s) for which it provides 35% of the U.S. domestic production capacity;
- Is the sole U.S. supplier;
- Produces a chemical or product used in the manufacture of defense weapons;

- Produces a chemical or product supplied to and for use by multiple defense weapons systems contractors;
- Is a major chemical supplier (>35% market share) to DoD for reasons other than defense weapons systems;
- Produces a chemical or product directly to another manufacturer, producer, or distributor for subsequent use in the manufacture of defense weapons systems;
- Serves as a major or sole supplier to a public health, water treatment, or power generation facility;

The Top-screen tool has the ability to calculate populations at risk and other potential consequences based upon factors such as geo-location and type and quantity of chemical without further information from the provider. The Top-screen tool will be part of a sophisticated system that allows the importation of data from the National Geospatial-Intelligence Agency (NGA) and other such data repositories, as well as the importation and use of modeling tools from the National Laboratories System. Accordingly, DHS will calculate consequentiality based upon the data that facilities provide during the Top-screen process.

APPENDIX B

Background:
Risk Analysis and Management for Critical Asset Protection (RAMCAP) Vulnerability Assessment Methodology

PREFACE

RAMCAP is an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework. RAMCAP was developed under contract to DHS by the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME).

As indicated, the Department is considering options for a vulnerability assessment tool for its chemical sector security program and invites comments on available options, including the elements of the process described below.

The Department thanks the Center for Chemical Process Safety (CCPS), the American Petroleum Institute (API), and the National Petrochemical & Refiners Association (NPRA) all of whom agreed to make their VA Methodology and other materials available to DHS as a reference to support the effort to produce a methodology that would support the Department's needs.

RAMCAP Vulnerability Assessment Methodology

General

The Risk Analysis and Management for Critical Asset Protection (RAMCAP) approach to risk analysis was developed for the Department to be broadly applicable to all critical infrastructure sectors. RAMCAP can assist with an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework. Phase 1 of the project developed the overall risk framework while Phase 2 was the further refinement and development of the methodologies at the sector level.

A Sector module includes 2 components – a screening process referred to as a Top-screen, and a vulnerability assessment tool, referred to as the VA.

1. The screening process provides a basis for understanding the critical infrastructures of greatest concern and the magnitude and nature of their significance. The DHS Top-screen to be employed in the implementation of regulations is described in general terms in Appendix A.

2. Vulnerability assessments will provide further vulnerability and consequence information based on several postulated threats of concern.

The threat scenarios to be used for RAMCAP were provided by DHS. The concept is as follows:

1. Each infrastructure would use the same threat scenarios
2. The user would begin by analyzing each of the scenarios on the list. If the facility cannot tolerate or neutralize this threat, or if a higher level of force causes a greater outcome, then the scenario would consider that greater force and analyze it.
3. The facility is not necessarily expected to be able to prevent or protect against the scenario.

This concept provides DHS with the information they require to make decisions about maximum expected consequences for each scenario. In this context, "threats" should be viewed as a yardstick employed to ascertain a consistent expression of vulnerability. These "threats" should not be seen as either indicative of government knowledge of enemy intent, nor as an expected design basis for security programs.

The RAMCAP methodology produces a relativistic expression of risk.

Objectives

The RAMCAP project creates a set of sector-specific vulnerability assessment tools that are:

- Consistent across sectors
- Appropriate to sector capabilities
- Reflective of asset owner/operator concerns, strengths and weaknesses
- Able to capture those datum points which support DHS information needs

The sector-specific vulnerability assessment tool being developed is:

- Based upon specific metrics, the use of which is repeatable sector to sector; thereby allowing cross-sector comparative risk assessment.
- Designed to employ specific, defined consequence generators (threat scenarios);
- Designed to evaluate:
    - Consequences (impact produced by the defined consequence generator);
    - Vulnerabilities (potential point targets and/or attack vectors, a broadly accepted surrogate for frequency/probability of success of an attack);
    - Countermeasures (including factors in mitigation, deterrent factors, detection factors, delay factors, response capability, and inherent robustness);
    - Actions/countermeasures at different threat levels;
    - Residual security vulnerability (gap analysis).

The purpose for a sector-specific assessment tool is to advance sector organization efforts to:

- Integrate key features of RAMCAP that cover Vulnerability Assessment (including threat and consequence analysis) into existing sector-specific methods, metrics and documentation, or;
- Assist sector organizations in developing new sector-specific Vulnerability Assessment methods, metrics and documentation as appropriate.

OVERVIEW OF THE RAMCAP VA METHODOLOGY

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

This step involves choosing appropriate threats for the SVA based on a DHS provided sector-level Threat Assessment of the potential threats to the critical infrastructure/key resource (CI/KR) sectors, as well as analysis of how those threats relate to sector vulnerabilities and consequences.

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 a higher consequence ranking value, 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 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 degree of threats assessed under Step 2, and the degree of vulnerability identified under Step 3.

Step 5: Countermeasures Analysis

Since RAMCAP is designed for use in a voluntary program wherein asset owners are only providing certain information to DHS, the asset owner is not required under RAMCAP to make security enhancements. However, within the DHS regulatory structure, the VA will lead directly to the production of a Site Security Plan, which must effectively address the vulnerabilities and risks identified in the VA. Accordingly, once the VA is completed, the team must make suggested recommendations to reduce security risks.

Based on the vulnerabilities identified and the risk that the layers of security are breached, appropriate enhancements to the security countermeasures are 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 VA report that can be used to communicate the results of the VA to management for appropriate action.

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 VA team’s recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Rejection of a VA recommendation and related acceptance of residual risk should be based on valid reasons that are well documented.

This VA process is summarized in Figure 1 and illustrated further in the flowcharts that follow in Figures 2a through 2c. Later in this chapter, preparation activities, such as data gathering and forming the VA team are described. Later sections provide details for each step in the RAMCAP VA methodology. These steps and associated tasks are also summarized in Figure 5.

Figure 1 — RAMCAP Vulnerability Assessment Methodology

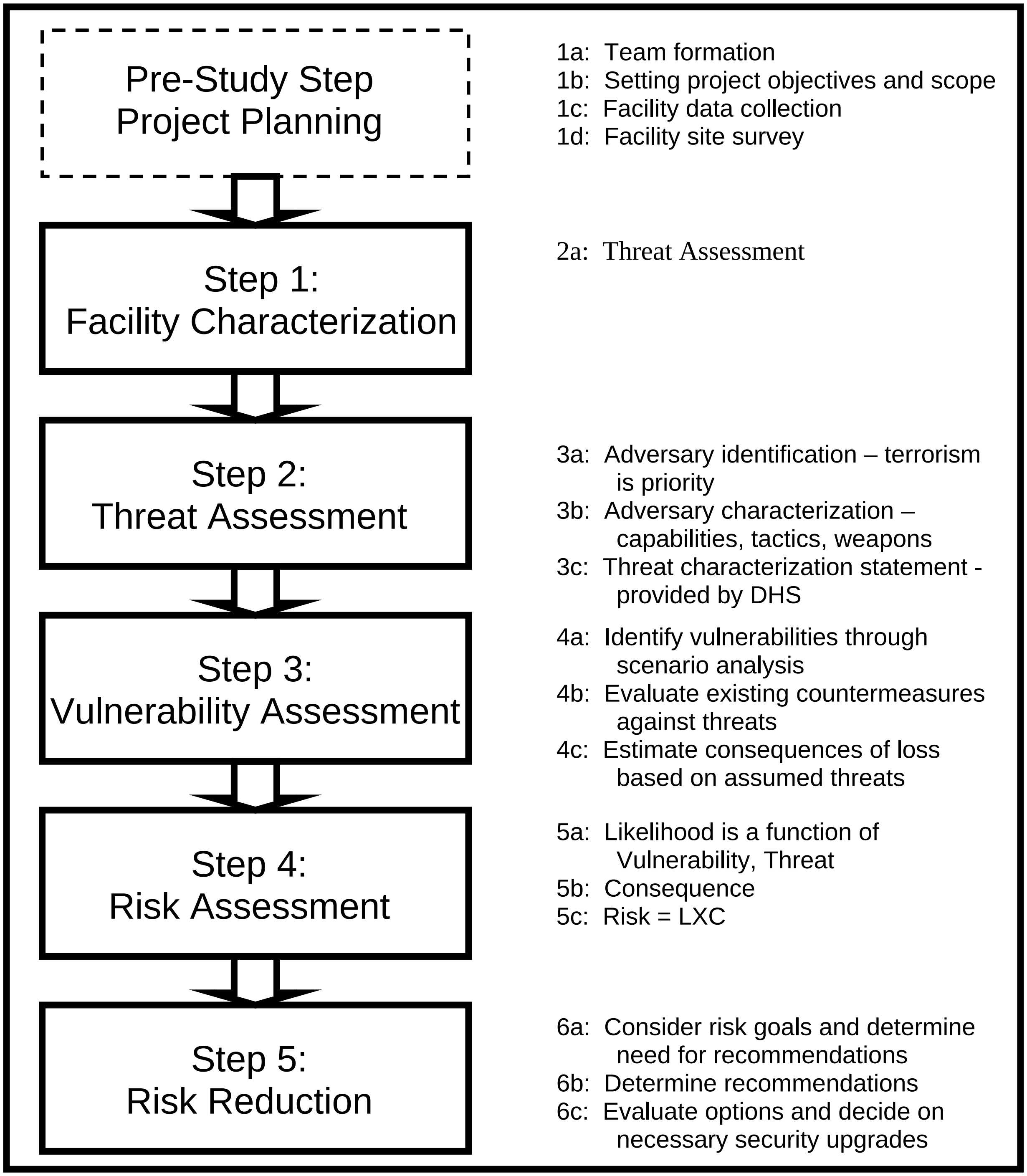

Pre-Study Step
Project Planning
1a: Team formation
1b: Setting project objectives and scope
1c: Facility data collection
1d: Facility site survey
Step 1:
Facility Characterization
2a: Threat Assessment
Step 2:
Threat Assessment
3a: Adversary identification – terrorism is priority
3b: Adversary characterization – capabilities, tactics, weapons
3c: Threat characterization statement - provided by DHS
Step 3:
Vulnerability Assessment
4a: Identify vulnerabilities through scenario analysis
4b: Evaluate existing countermeasures against threats
4c: Estimate consequences of loss based on assumed threats
Step 4:
Risk Assessment
5a: Likelihood is a function of Vulnerability, Threat
5b: Consequence
5c: Risk = LXC
Step 5:
Risk Reduction
6a: Consider risk goals and determine need for recommendations
6b: Determine recommendations
6c: Evaluate options and decide on necessary security upgrades

Figure 2a—RAMCAP Vulnerability Assessment Methodology—Step 1

API/NPRA Security Vulnerability Analysis Methodology - Step 1

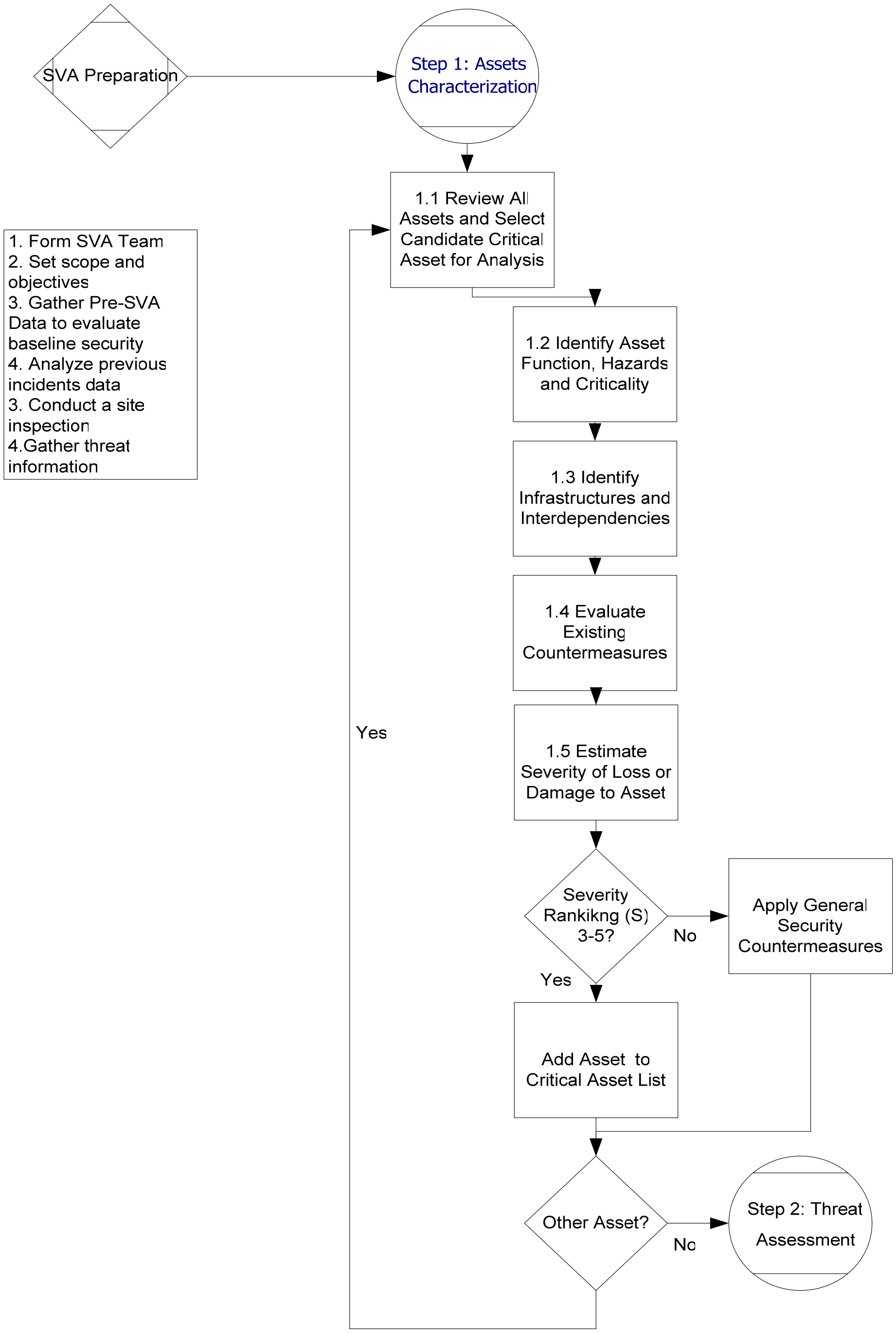
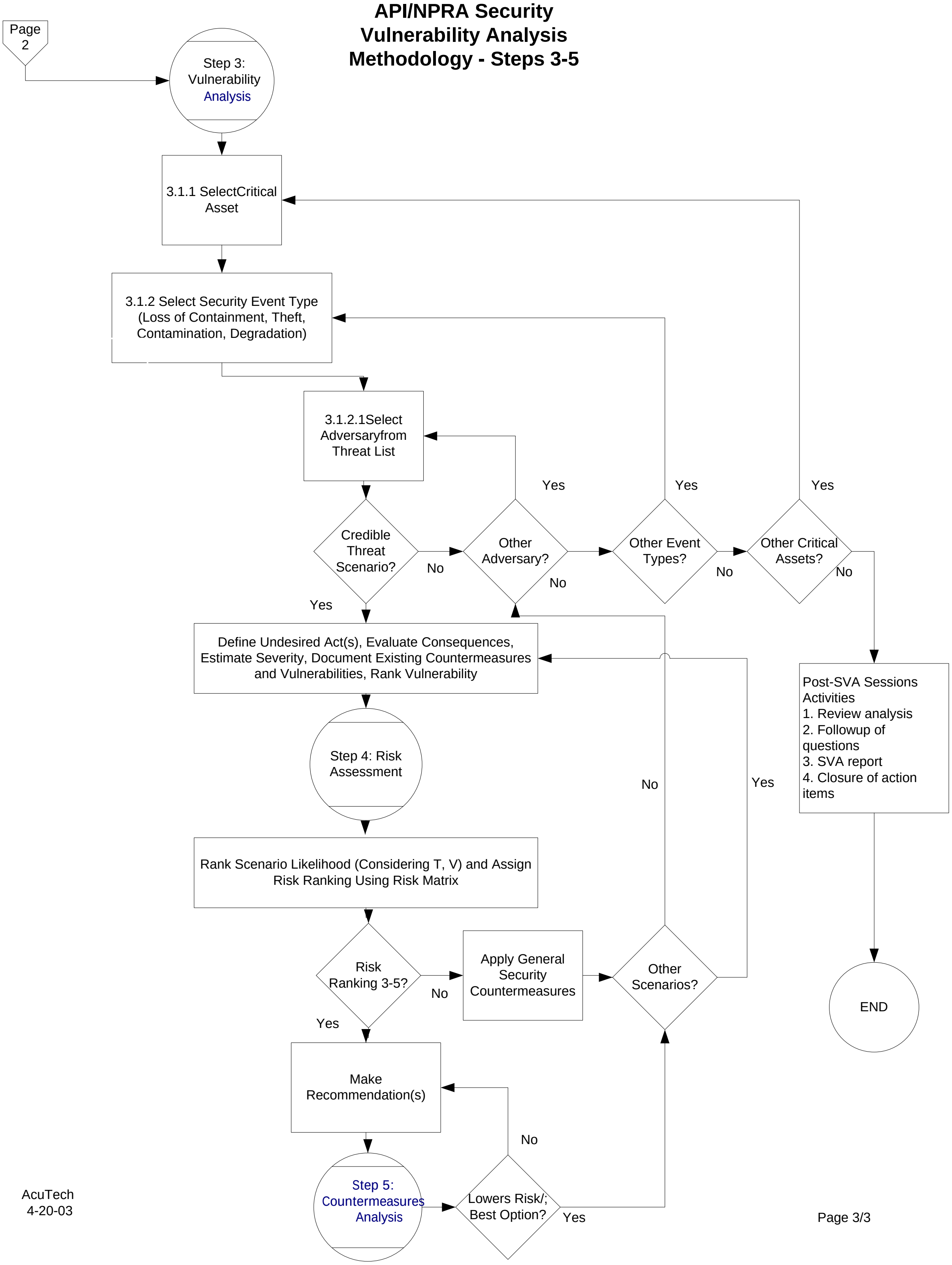

SVA Preparation
Step 1: Assets Characterization
1.1 Review All Assets and Select Candidate Critical Asset for Analysis
1. Form SVA Team
2. Set scope and objectives
3. Gather Pre-SVA Data to evaluate baseline security
4. Analyze previous incidents data
3. Conduct a site inspection
4.Gather threat information
1.2 Identify Asset Function, Hazards and Criticality
1.3 Identify Infrastructures and Interdependencies
1.4 Evaluate Existing Countermeasures
Yes
1.5 Estimate Severity of Loss or Damage to Asset
Severity Rankikng (S) 3-5?
No
Apply General Security Countermeasures
Yes
Add Asset to Critical Asset List
Other Asset?
No
Step 2: Threat Assessment

Figure 2b—RAMCAP Vulnerability Assessment Methodology—Step 2

Details of the Threat Assessment portion of the methodology are still being developed.

Figure 2c—RAMCAP Vulnerability Assessment Methodology—Steps 3–5

API/NPRA Security Vulnerability Analysis Methodology - Steps 3-5


Page 2
Step 3: Vulnerability Analysis
3.1.1 SelectCritical Asset
3.1.2 Select Security Event Type (Loss of Containment, Theft, Contamination, Degradation)
3.1.2.1Select Adversaryfrom Threat List
Credible Threat Scenario?
No
Yes
Other Adversary?
Yes
No
Other Event Types?
Yes
No
Other Critical Assets?
Yes
No
Define Undesired Act(s), Evaluate Consequences, Estimate Severity, Document Existing Countermeasures and Vulnerabilities, Rank Vulnerability
Step 4: Risk Assessment
Rank Scenario Likelihood (Considering T, V) and Assign Risk Ranking Using Risk Matrix
Risk Ranking 3-5?
No
Yes
Apply General Security Countermeasures
Other Scenarios?
No
Yes
Make Recommendation(s)
Step 5: Countermeasures Analysis
Lowers Risk/; Best Option?
No
Yes
Post-SVA Sessions Activities
1. Review analysis
2. Followup of questions
3. SVA report
4. Closure of action items
END

AcuTech
4-20-03

Page 3/3

VA METHODOLOGY

Planning for Conducting an VA

Prior to conducting the VA 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 an VA including the following:

- the activity should be planned 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 VA process methodology.

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

Prerequisites to conducting the VA 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.

VA Team

The VA 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 site security plan. The primary goal of this group is to capture and build into the VA method the experience of this diverse group of individual experts so that the VA process will capture and incorporate information that may not be available in typical operator databases.

If the VA will include terrorism attacks on a process handling flammable, explosive, reactive or toxic substances, the VA 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 likely to be 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, VA teams should possess the knowledge and/or skills listed in Figure 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 VA 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 VA approach.

VA Objectives and Scope

The VA Team Leader should develop an objectives and scope statement for the VA. This helps to focus the VA and ensure completeness. An example VA objectives statement is shown in Figure 4.

A work plan should then be developed to conduct the VA 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 harm to critical infrastructure that may result in catastrophic consequences. For the RAMCAP methodology, the key events and consequences of interest include those described as key security events in the CCPS VA guidelines.[7] In addition to the security events recommended in those guidelines, the RAMCAP VA methodology recommends including injury to personnel and the public directly or indirectly.

Other events may be included in the scope, but it is prudent to address these four primary security events first since these are primarily events involving the processes that make the petroleum industry facilities unique from other facilities.

Figure 3 — RAMCAP VA Team Members

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

- Team Leader – knowledge of and experience with the VA 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 VA 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 4 — VA Sample Objectives Statement

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.

Figure 5 — RAMCAP VA Methodology, 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.

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.

Annex 1 includes a list of potentially useful data that may be needed to conduct an VA.

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).

Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the VA methodology selected, and the decisions that are to be made. The data collection approach will follow the VA path determined by the initial expert team assembled to identify the data needed for the first pass at VA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the VA 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 VA. As the VA process evolves, the scope of the data collection will be expanded to support more detailed assessment of perceived areas of vulnerability.

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 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

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

Analyzing Previous Incidents Data

Any previous security incidents relevant to the 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.

Conducting a Site Inspection

Prior to conducting the VA 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.

Gathering Threat Information

The team should gather and analyze relevant company and industry and DHS (or other governmental) provided threat information, such as that available from the Energy ISAC, DHS, FBI, or other local law enforcement agency. At a minimum, the DHS-provided Threat Handbook should be thoroughly reviewed by all team members.

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. This factor (severity of the consequences) is 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 6 below summarizes the key steps and tasks required for Step 1.

Step 1.1 – Identify Critical Assets

The VA 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. Assets include the full range of both material and non-material aspects that enable a facility to operate.

Figure 6 — RAMCAP VA Methodology, 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 7 — RAMCAP VA Methodology, 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 VA 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 VA 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 VA 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 VA 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-VA survey is helpful to gather this information. The data will be made available to the VA 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.

A 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. An example is included in Attachment 1

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. Annex 2 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).

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 VA 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 Annex 1 - 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 the selection listed in Figure 8. For DHS purposes, an VA will consider the consequences shown in Figure 9.

Figure 8—RAMCAP VA Methodology,

Selected Possible Consequences of RAMCAP VA Security Events

Public fatalities or injuries
Site personnel fatalities or injuries
Large-scale disruption to the national economy, public or private operations
Loss of reputation or business viability

Figure 9 **Modified RAMCAP Consequence Parameters**
1. Human Health & Safety Impacts
a. Reported estimated residential population within the distance to the RMP toxic and flammable WCS endpoints (where EPA RMP is applicable)
b. Acute fatalities

c. Acute injuries
d. Theft of chemical weapons precursors/weapons of mass destruction onsite
e. Contamination to final food or pharmaceutical products made onsite
2. Economic Impacts
3. National Security & Government Functionality Impacts
a. Military mission importance
b. Delivery of public health services
c. Contamination/disruption to critical potable water or electrical energy services
4. Psychological Impacts
a. Impact to iconic/symbolic assets
b. High profile and/or symbolic casualties

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 10 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. Asset owners may consider using a risk matrix such as this for making individual risk-based decisions for security, particularly if they use the

RAMCAP VA methodology as a generalized vulnerability assessment tool.

Figure 10 — RAMCAP VA Methodology, 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. Between $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. Between $X -$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. Between $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

As part of the RAMCAP program, DHS has been interested in certain consequence and vulnerability information for a limited number of more critical national sites. For reporting this information to DHS, the following ranking process should be used for assessing consequences.

Figure 11
RAMCAP Consequence Ranges

RAMCAP Consequence Criteria	**Consequence Categories**										
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Number Of Fatalities	0 - 100	101 - 200	201 – 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400
Number Of Injuries	0 - 300	501 - 1000	1001 - 2000	2001 - 4000	4001 - 8000	8001 - 16000	16001 - 32000	32001 - 64000	64001 - 128000	128001 - 256000	256001 - 512000
Economic Impacts	<$100M	$100M - $200M	$200M - $400M	$400M - $800M	$800M - $1.6B	$1.6B - $3.2B	$3.2B - $6.4B	$6.4B - $12.8B	$12.8B - $25.6B	$25.6B - $51.2B	$51.2B - $102.4B

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 VA. The economic consequences for RAMCAP include direct replacement costs, business interruption, and the cost of cleanup and restoration.

The VA Team should evaluate the potential consequences of an attack using the judgment of the VA 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.

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 VA Team develops a Target Asset List that is a list of the assets associated with the site being studied that are more likely to be 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 RAMCAP VA methodology uses ranking systems that are based on a scale of 1-5 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.

STEP 2: THREAT ASSESSMENT

This step involves identifying appropriate threat scenarios for the SVA based on a DHS provided sector-level Threat Assessment that provides an overall assessment of the potential threats to the CI/KR sectors, as well as analysis of how these threats relate to sector vulnerabilities and consequences.

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.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets. It supports the establishment and prioritization of security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability and intent.

The assessment should identify threat categories and potential adversaries, such as insiders, external agents (outsiders), and collusion between insiders and outsiders. The SVA team should consider each type of adversary identified in the threat assessment and their assessed level of capability and motivation.

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.

Examples of threats are set forth on the following table (Fig. 12):

Readers are advised: the RAMCAP postulated threats, developed by and currently in use by industry, are for illustrative purposes only. Certain threats set forth below would not be applicable to the chemical security program at issue.

Figure 12
RAMCAP Postulated Threat Scenarios

Maritime (Boat as weapon)				
1. Delivery	Small boat (pleasure or Zodiac) <10ft draft	Fast Boat <10 ft draft	Barge	Deep draft shipping 20-40 ft draft
Explosive	Explosive charge 400 lbs TNT equivalent	Explosive charge 2000 lbs (TNT equivalent)	Explosive charge -10000 lbs (TNT equivalent)	Explosive charge 40,000 lbs (TNT equivalent) LNG, LPG, weaponized

Land VBIED (w/out assault team)				
2. Single VBIED	Car bomb 400lbs TNT equivalent	Van Bomb 1000lbs TNT equivalent	Mid-size Truck Bomb 10,000lbs TNT equivalent	Large Truck Bomb (18 wheeler) 40,000lbs TNT equivalent
What do they do? Attempt to maximize death/destruction through most productive direct means. For example, aiming at critical assets in hard targets, or clusters of people for open populated areas, or structural supports that would bring down people.				

Assault				
Assault force size	1	2-4	5-8	9-16
3. Delivery system **"Land"**	Pedestrian, all-terrain vehicle, motorcycle, over the road personnel transport, cargo truck	All-terrain vehicles, motorcycles, over the road personnel transport, cargo truck	All-terrain vehicles, motorcycles, over the road personnel transport, cargo truck,	All-terrain vehicles, motorcycles, over the road personnel transport, Cargo truck,
4. Delivery system **"Air"**	N/A	1 Helicopter Pilot + 1-3 attack force	2 Helicopters 2 pilots + 4-6 attack force	3 Helicopters 3 pilots + 7-13 attack force
5. Delivery	Lone swimmer	1 x small boat	1 x small boat (Zodiac)	2 x small boat Zodiac

Figure 12
RAMCAP Postulated Threat Scenarios

system **“Water”**		(Zodiac)	(personnel) 1 x small/medium cargo watercraft (equipment)	Medium cargo watercraft (equipment)
Weapons	Pistol, assault rifle, light machine gun	Pistols, assault rifles, sniper rifles (.50 caliber), light machine guns	Pistols, submachine guns, assault rifles, sniper rifles (.50 caliber), light machine guns, rocket propelled grenades (RPG)	Pistols, submachine guns, assault rifles, sniper rifles (.50 caliber), light machine guns, rocket propelled grenades (RPG)
Explosives	Grenades (H.E. & Incendiary) Explosive vest/or satchel.	Grenades (H.E. & Incendiary) Bulk explosives, VBIED (400lb TNT equivalent) for access or attack	Grenades (H.E. & Incendiary) Bulk explosives, VBIED (400lb TNT equivalent) for access or attack Specialized Explosive charges (Breaching charges, shape charges, ballistic discs)	Grenades (H.E. & Incendiary) Bulk explosives, 2 VBIEDs (400lb TNT equivalent) for access or attack Specialized Explosive charges (Breaching charges, shape charges, ballistic discs) Anti-personnel mines
Tools	Minimal breaching tools	Mechanical breaching tools, required hand tools	Mechanical breaching tools, quick saws, chainsaws, sledge hammers, required hand tools	Mechanical breaching tools, quick saws, chainsaws, sledge hammers, required hand tools
Weight per person	65 pounds	65 pounds	65 pounds	65 pounds
What do they do inside? Attempt to maximize death/damage through most productive direct means. For example, in a nuclear plant, they try to achieve sabotage the reactor and breach containment. For the mall, they try to kill as many as possible directly. Assume suicide intent.				
Process Sabotage				
7. Cyber				
8. Insider threat				
9. Unauthorized access				
What do they do? Cause harm through process control systems, though contamination, etc.				
Diversion of sensitive property (theft)				
10. Cyber				
11.Insider threat				
12. Unauthorized access				
What do they do? Steal information, dangerous substances, valuable resources, etc.				

The threat assessment is not based on perfect information and will be developed in the absence of site-specific information on threats. A suggested approach is to make an assumption that international terrorism is possible at every facility.

VA STEP 3: VULNERABILITY ANALYSIS

The Vulnerability Analysis step involves three steps. Once the VA 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 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 13 — RAMCAP VA Methodology, Description of Step 3 and Sub-steps

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 RAMCAP VA Methodology - 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 VA 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 VA 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 VA 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 14. For RAMCAP purposes, the asset owner also is asked to evaluate the likelihood of successful attack against the prescribed postulated threat scenarios at a minimum using the definitions shown in Figure 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 VA 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 RAMCAP VA Methodology – Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form.

Figure 14 — RAMCAP VA Methodology, 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.

Figure 15 RAMCAP Vulnerability vs. Consequences Matrix

	Descriptor	Range	Representative Likelihood	Cat	CONSEQUENCE CATEGORIES										
					0	1	2	3	4	5	6	7	8	9	10
VULNERABILITY (Likelihood of Adversary Success)	Adversary is almost certain to succeed	0.5 - 1	> 50/50	5											
	Adversary's chances of success about even	0.25 - 0.5	~1 in 3	4											
	Adversary might succeed - but less than 50/50 chance	0.125 - 0.25	~1 in 5	3											
	Adversary is probably not going to succeed	0.0625 - 0.125	~1 in 10	2											
	Extremely Unlikley	0.0312 - 0.0625	~1 in 20	1											
	Ext Impossible	<0.0312	< 1 in 50	0											
Number Of Fatalities					0 - 100	101 - 200	201 - 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400
Number Of Injuries					0 - 300	501 - 1000	1001 - 2000	2001 - 4000	4001 - 8000	8001 - 16000	16001 - 32000	32001 - 64000	64001 - 128000	128001 - 256000	256001 - 512000
Economic Impacts					<$100M	$100M - $200M	$200M - $400M	$400M - $800M	$800M - $1.6B	$1.6B - $3.2B	$3.2B - $6.4B	$6.4B - $12.8B	$12.8B - $25.6B	$25.6B - $51.2B	$51.2B - $102.4B

The VA 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 earlier, the four types of security events included in the objectives of an VA 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, 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 VA team brainstorms the vulnerabilities based on the information collected in Steps 1-3. The VA 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 VA 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. 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.
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 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.

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 16 lists the sub-steps.

The scenarios are risk-ranked by the VA Team based on a simple scale of 1-5. The risk matrix shown in Figure 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 VA 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 16 — RAMCAP VA Methodology, 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 17 — RAMCAP VA Methodology, Risk Ranking Matrix

SEVERITY						
		5	**4**	**3**	**2**	**1**
LIKELIHOOD	**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 18 — RAMCAP VA Methodology, 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

FOLLOW-UP TO THE VA

The outcome of the VA is:

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

The VA 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 VA 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 RAMCAP VA Methodology Forms

The following four forms can be used to document the VA 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 VA guidance can be used.

Step 1: RAMCAP VA Methodology - Critical Assets/Criticality Form

Facility Name:

Critical Assets	**Criticality/Hazards**	**Asset Severity Ranking**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

9.		

Step 3-5: RAMCAP VA Methodology – Vulnerability Analysis/Risk Ranking/Countermeasures Form

Facility Name:

Critical Assets:

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 VA 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 to be used 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 be considered involve those that are extremely severe. Some examples of relevant consequences in an VA 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 intent, and capabilities 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.

Vulnerability Assessment (VA): An VA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. VAs 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 VA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

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

ACC	American Chemistry Council
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
RAMCAP	Risk Analysis and Management for Critical Asset Protection
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
T	Threat
TSA	Transportation Security Administration
V	Vulnerability
VA	Vulnerability Assessment
WMD	Weapons of Mass Destruction

ANNEX A — VA Supporting Data Requirements

RAMCAP VA 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 an VA 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 VA team as much in advance as possible before arrival for familiarization;

B = Documentation to be gathered for use in VA team meetings on site;

C = Documentation that should be readily available on an as-needed basis.

Acknowledgements

“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.

APPENDIX C

Title 33: Navigation and Navigable Waters

*** * ***

PART 105—MARITIME SECURITY: FACILITIES

§ 105.250   Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in §105.225 of this subpart.

(c) The FSP must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 105.255   Security measures for access control.

(a) General. The facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility; and

(3) Control access to the facility.

(b) The facility owner or operator must ensure that the following are specified:

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level. Each location allowing means of access to the facility must be addressed;

(2) The identification of the type of restriction or prohibition to be applied and the means of enforcing them;

(3) The means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without challenge; and

(4) The identification of the locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

(c) The facility owner or operator must ensure that an identification system is established for checking the identification of facility personnel or other persons seeking access to the facility that:

(1) Allows identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems of vessels or other transportation conveyances that use the facility;

(3) Is updated regularly;

(4) Uses disciplinary measures to discourage abuse;

(5) Allows temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identity; and

(6) Allows certain long-term, frequent vendor representatives to be treated more as employees than as visitors.

(d) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) MARSEC Level 1. The facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter;

(3) Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors. This check includes confirming the reason for entry by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system required in paragraph (c) of this section;

(4) Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel, to establish his or her identity or to account for his or her presence. Any such incident must be reported in compliance with this part;

(5) Designate restricted areas and provide appropriate access controls for these areas;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(8) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(9) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(f) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(g) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage;

(3) Being prepared to cooperate with responders and facilities;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

§ 105.260 Security measures for restricted areas.

(a) General. The facility owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be in the facility;

(3) Protect the facility;

(4) Protect vessels using and serving the facility;

(5) Protect sensitive security areas within the facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect cargo and vessel stores from tampering.

(b) Designation of Restricted Areas. The facility owner or operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

(1) Shore areas immediately adjacent to each vessel moored at the facility;

(2) Areas containing sensitive security information, including cargo documentation;

(3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(4) Areas containing critical facility infrastructure, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Electrical system; and

(iv) Access points for ventilation and air-conditioning systems;

(5) Manufacturing or processing areas and control rooms;

(6) Locations in the facility where access by vehicles and personnel should be restricted;

(7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

(1) Identify which facility personnel are authorized to have access;

(2) Determine which persons other than facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply;

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) MARSEC Level 1. At MARSEC Level 1, the facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Assigning personnel to control access to restricted areas;

(4) Verifying the identification and authorization of all persons and all vehicles seeking entry;

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

(e) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;

(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;

(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(4) Restricting parking adjacent to vessels;

(5) Further restricting access to the restricted areas and movements and storage within them;

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and restricting access to areas adjacent to the restricted areas.

(f) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas, or

(3) Searching restricted areas as part of a security sweep of all or part of the facility.

§ 105.275 Security measures for monitoring.

(a) General. The facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the:

(1) Facility and its approaches, on land and water;

(2) Restricted areas within the facility; and

(3) Vessels at the facility and areas surrounding the vessels.

(b) MARSEC Level 1. At MARSEC Level 1, the facility owner or operator must ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility, ensure monitoring capability that:

(1) When automatic intrusion-detection devices are used, activates an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;

(3) Monitors the facility area, including shore and waterside access to it;

(4) Monitors access points, barriers and restricted areas;

(5) Monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and

(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(c) MARSEC Level 2. In addition to the security measures for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional measures may include:

(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;

(2) Increasing the frequency of foot, vehicle or waterborne patrols;

(3) Assigning additional security personnel to monitor and patrol; or

(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must also ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Switching on all lighting within, or illuminating the vicinity of, the facility;

(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility;

(3) Maximizing the length of time such surveillance equipment can continue to record; or

(4) Complying with the instructions issued by those responding to the security incident.

§ 105.280 Security incident procedures.

For each MARSEC Level, the facility owner or operator must ensure the Facility Security Officer and facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;

(b) Evacuate the facility in case of security threats or breaches of security;

(c) Report security incidents as required in §101.305 of this subchapter;

(d) Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Secure non-critical operations in order to focus response on critical operations.