

**DRAFT**

**VULNERABILITY ASSESSMENT  
METHODOLOGY**

**Electric Power Infrastructure**



**U.S. Department of Energy  
Office of Energy Assurance**

**September 30, 2002**

## CONTENTS

1	Introduction .....	4
2	Vulnerability Assessment Process .....	7
3	Pre-Assessment .....	9
4	Vulnerability Assessment Methodology .....	13
5	Post-Assessment.....	20
	Appendix A: Critical Assets Methodology.....	21
	Appendix B: Request for Information .....	27
	Appendix C: Vulnerability Survey Methodology.....	40

## FIGURES

2.1	Vulnerability Assessment Phases.....	8
3.1	Example Risk Management Process .....	11
C.10.1	Estimating Expected Damage to Assets.....	154

## TABLES

A.1	Criticality/Consequence Dimensions and Attributes .....	23
A.2	Critical Asset Listing.....	25
C.2.1	List of Organizations to Contact for Threat Information .....	43
C.4.1	Physical Security Program .....	56
C.4.2	Physical Security Barriers .....	57
C.4.3	Physical Security Access Control/Badges.....	58
C.4.4	Physical Security Locks/Keys.....	59
C.4.5	Physical Security Intrusion Detection Systems.....	60
C.4.6	Physical Security Communications Equipment .....	63
C.4.7	Protective Force/Local Law Enforcement Agency .....	64
C.4.8	Entrances into Critical Asset Areas.....	65
C.4.9	Surfaces Surrounding Critical Asset Areas.....	68
C.4.10	Fences Surrounding Critical Asset Areas.....	72
C.4.11	Vehicle Gates through Critical Asset Area Fences .....	74
C.6.1	Human Resources Security Procedures.....	81
C.6.2	Facility Engineering .....	83
C.6.3	Facility Operations .....	85
C.6.4	Administrative Support Organizations.....	87
C.6.5	Telecommunications and Information Technology .....	89
C.6.6	Publicly Released Information .....	91
C.6.7	Trash and Waste Handling .....	93
C.7.1	List of Interview Candidates for Policies and Procedures Element.....	95
C.8.1	Estimates of Unit Costs of Outages.....	98
C.8.2	Estimated Value of a Utility Energy 24-hour Outage .....	98
C.9.1	Infrastructure Oversight and Procedures.....	102

## TABLES (Cont'd.)

C.9.2	Electric Power Supply and Distribution.....	104
C.9.3	Petroleum Fuels Supply and Storage .....	105
C.9.4	Natural Gas Supply .....	106
C.9.5	Telecommunications .....	107
C.9.6	Transportation .....	108
C.9.7	Water and Water System.....	109
C.9.8	Emergency Services .....	110
C.9.9	Internal Computers and Servers .....	111
C.9.10	HVAC System.....	112
C.9.11	Fire Suppression and Fire Fighting System .....	113
C.9.12	SCADA System.....	114
C.9.13	Physical Security System .....	115
C.9.14	Financial System .....	116
C.10.1	Asset Attractiveness Scale .....	146
C.10.2	Level of Consequence Scale .....	147
C.10.3	Technical and Cultural Difficulty Scale.....	148
C.10.4	Dependency on Other Infrastructures Scale.....	148
C.10.5	Risk Characterization of Recommendations .....	149
C.10.6	Categorization of Recommendations .....	149
C.10.7	Lowest-cost Recommendations.....	150
C.10.8	Recommendations with the Largest Increases in Probability of Preventing an Aggressor Attempt.....	151
C.10.9	Recommendations with the Largest Increases in Probability of Preventing Aggressor Success, Given an Attempt Is Not Prevented .....	151
C.10.10	Recommendations that Address Extremely Attractive Assets.....	151
C.10.11	Recommendations that Address High-consequence Assets.....	152

# 1 INTRODUCTION

## 1.1 OBJECTIVE

Effective operation of the U.S. energy infrastructure—the electric power, oil, and natural gas production, transmission, and distribution systems that fuel and power our economy—is critical to the health and safety, national security, and economic viability of our nation. As the lead agency for the energy industry, the U.S. Department of Energy (DOE) is increasingly concerned about the reliability and security of this critical infrastructure and, in particular, about the possibility of terrorist attacks that could target that infrastructure. The possibility of terrorist attacks is especially problematic in the post-September 11<sup>th</sup> world.

This report is an update to “*Vulnerability and Risk Analysis Program: Overview of Assessment Methodology*,” September 28, 2001. The initial report provided a high-level overview of the vulnerability assessment methodology being developed and validated by DOE’s Office of Energy Assurance (OEA) as part of its multifaceted mission to work with the energy sector in developing the capability required to protect our nation’s energy infrastructures. This updated report focuses specifically on a methodology that has been applied to the electric power infrastructure and at a more detailed level. Over the last five years, a team of national laboratory experts, working in partnership with the energy industry, has successfully applied the methodology as part of OEA’s Vulnerability Assessment Program (VAP) to help energy-sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures. Lessons learned from these assessments, as well as best practice approaches to mitigate vulnerabilities, are being continuing to be documented in related reports.

The purpose of this report is to provide a methodology resource for the electric power industry. No one vulnerability assessment methodology has all the answers. Companies should consider for themselves the applicability of the vulnerability assessment elements to their individual situation. Each company should determine which elements are applicable (if any) along with the appropriate level of detail.

## 1.2 BACKGROUND

The primary mission of OEA is to work with the national energy sector in developing the capability required for assuring the nation’s energy infrastructures. This mission encompasses the physical and cyber components of the electric power, oil, and natural gas infrastructures, the interdependencies among these components, and the interdependencies with the other critical national infrastructures. The mission also includes identifying DOE technologies and capabilities that can help assure our nation’s critical energy infrastructures and facilitating their use by the private sector and other federal agencies.

VAP is an integral part of the overall OEA strategy in critical infrastructure protection where the Department, as the federal government lead agency for the energy sector, partners with industry to address vital issues of mutual interest. The specific objective of the program is to partner with

the energy industry (electric power, oil, and natural gas) to “develop and implement a vulnerability awareness and education program for their sector” to enhance the security of the energy infrastructure, as directed by PDD-63. To accomplish the mission, the program is designed to develop, validate, and disseminate assessment and survey methodologies with associated tools to assist in the implementation; provide training and technical assistance; and stimulate action to mitigate significant problems.

Fourteen vulnerability assessments (and 20 vulnerability surveys/quick-turnaround assessments) have been completed under this initiative (several more are in progress and in the planning stages). To date, 13 of the vulnerability assessments and 10 of the vulnerability surveys have focused on the electric power infrastructure. Facilities examined included generation, transmission, and distribution facilities along with independent system operators. Assessments addressed key energy organizations whose operations, if disrupted, would have broad regional or national impact. This report presents the methodology that was performed on these electric power facilities.

### 1.3 REPORT ORGANIZATION

The remainder of this report is organized as follows. Section 1.4 discusses the benefits of vulnerability assessments and surveys. Section 2 discusses the motivation for the Vulnerability Assessment Program and provides an overview of the three steps in the assessment process—pre-assessment, assessment, and post-assessment. Sections 3, 4, and 5 discuss each of these steps.

### 1.4 BENEFITS OF ASSESSMENTS

Energy utilities should routinely perform vulnerability assessments to better understand threats and vulnerabilities, determine acceptable levels of risk, and stimulate action to mitigate identified vulnerabilities. The direct benefits of performing a vulnerability assessment include:

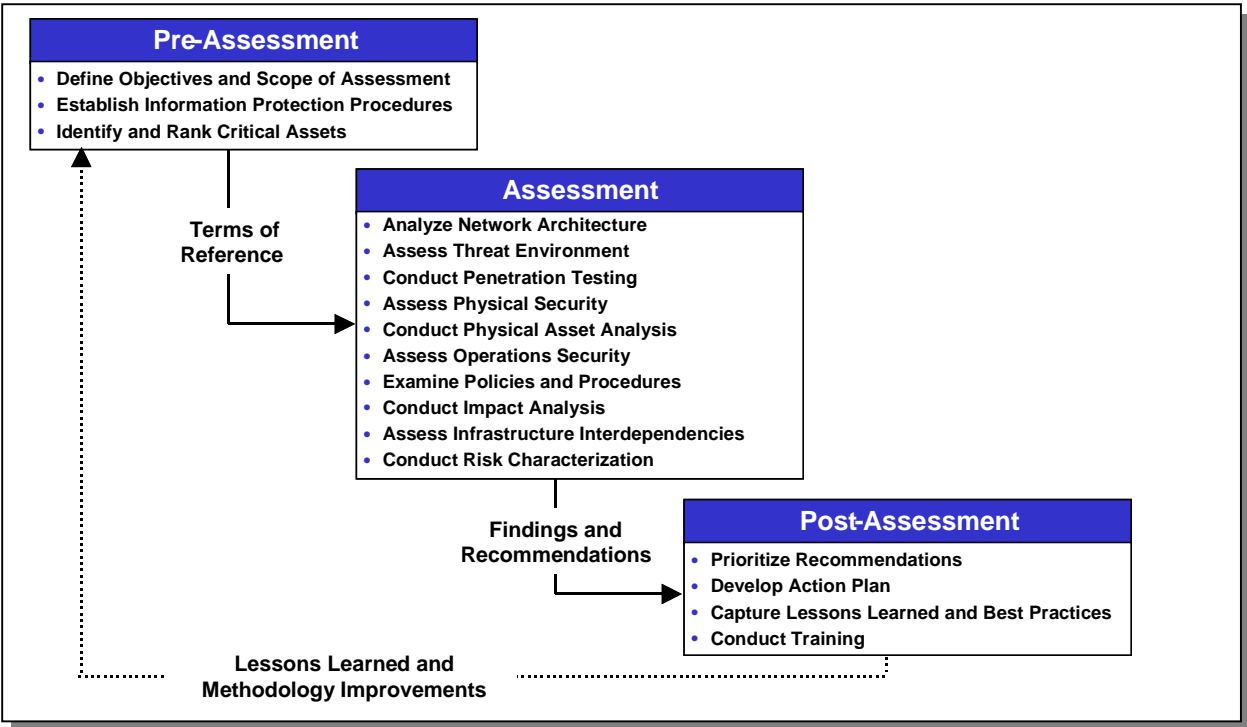
- **Build and broaden awareness.** The assessment process directs senior management’s attention to security. Security issues, risks, vulnerabilities, mitigation options, and best practices are brought to the surface. Awareness is one of the least expensive and most effective methods for improving the organization’s overall security posture.
- **Establish or evaluate against a baseline.** If a baseline has been previously established, an assessment is an opportunity for a checkup to gauge the improvement or deterioration of an organization’s security posture. If no previous baseline has been performed (or the work was not uniform or comprehensive), an assessment is an opportunity to integrate and unify previous efforts, define common metrics, and establish a definitive baseline. The baseline also can be compared against best practices to provide perspective on an organization’s security posture.

- **Identify vulnerabilities and develop responses.** Generating lists of vulnerabilities and potential responses is usually a core activity and outcome of an assessment. Sometimes, due to budget, time, complexity, and risk considerations, the response selected for many of the vulnerabilities may be non-action, but after completing the assessment process, these decisions will be conscious ones, with a documented decision process and item-by-item rationale available for revisiting issues at scheduled intervals. This information can help drive or motivate the development of a risk management process.
- **Categorize key assets and drive the risk management process.** An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key assets. This ranking, combined with threat, vulnerability, and risk analysis, is at the heart of any risk management process. For many organizations, the Y2K threat was the first time a company-wide inventory and ranking of key assets was attempted. An assessment allows an organization to revisit that list from a broader and more comprehensive perspective.
- **Develop and build internal skills and expertise.** A security assessment, when not implemented in an “audit” mode, can serve as an excellent opportunity to build security skills and expertise within an organization. A well-structured assessment can have elements that serve as a forum for cross-cutting groups to come together and share issues, experiences, and expertise. External assessors can be instructed to emphasize “teaching and collaborating” rather than “evaluating” (the traditional role). Whatever an organization’s current level of sophistication, a long-term goal should be to move that organization toward a capability for self-assessment.
- **Promote action.** Although disparate security efforts may be underway in an organization, an assessment can crystallize and focus management attention and resources on solving specific and systemic security problems. Often the people in the trenches are well aware of security issues (and even potential solutions) but are unable to convert their awareness to action. An assessment provides an outlet for their concerns and the potential to surface these issues at appropriate levels (legal, financial, executive) and achieve action. A well-designed and executed assessment not only identifies vulnerabilities and makes recommendations, it also gains executive buy-in, identifies key players, and establishes a set of cross-cutting groups that can convert those recommendations into action.
- **Kick off an ongoing security effort.** An assessment can be used as a catalyst to involve people throughout the organization in security issues, build cross-cutting teams, establish permanent forums and councils, and harness the momentum generated by the assessment to build an ongoing institutional security effort. The assessment can lead to the creation of either an actual or a virtual (matrixed) security organization.

## 2 VULNERABILITY ASSESSMENT PROCESS

Figure 2.1 provides an overview of the assessment methodology. As shown, the methodology is divided into three basic phases: pre-assessment, assessment, and post-assessment. Each phase consists of a series of elements or tasks that have been designed by the VAP team of national laboratory experts. Lessons learned have been captured and used to enhance and, when appropriate, expand the methodology. The specific elements or tasks associated with each assessment phase can be tailored to meet specific assessment objectives. Although the methodology has incorporated unique elements that leverage the expertise of the national laboratories, the methodology can be adapted for self-assessment.

A number of assessment techniques, methods, and approaches used by other organizations (public and private-sector) have been examined in developing the methodology shown in Figure 2.1. This includes information gathered through open literature, presentations, classroom instructions, and discussions. In addition, elements of the methodology have been derived from ongoing DOE security and infrastructure assurance programs. In particular, the significant investment by DOE in the development of policies, procedures, processes, and technologies to solve the challenge of protecting the nation's most sensitive information and special nuclear materials has provided a foundation for this initiative. The basic VAP philosophy is to leverage vulnerability assessment techniques, methods, and approaches that have proven to be useful and useable.



**Figure 2.1 Vulnerability Assessment Phases**

## 3 PRE-ASSESSMENT

The pre-assessment phase involves defining the scope of the assessment, establishing appropriate information protection procedures, and identifying and ranking critical assets. Each of these activities is critical in ensuring the success of the assessment.

### 3.1 SCOPE OF ASSESSMENT

A wide range of activities are involved in defining the scope of the assessment. These include identifying the assessment objectives and measures of success, specifying the elements of the methodology that will be included in the assessment, engaging knowledgeable personnel and ensuring access to resources and information, deciding on the type of assessment (internal, facilitated, external, hybrid) to be conducted, and developing an assessment schedule.

Assessment objectives and measures of success define the assessment and must be tailored to the organization. Possible objectives include the following:

- Identify all critical vulnerabilities—physical, cyber, and interdependencies—and develop appropriate response options.
- Identify and rank all key assets from a security perspective.
- Develop the business case for making security investments and organizational changes that will enhance security.
- Enhance awareness and make security an integral part of the business strategy.

The process of setting the assessment objectives will help to define the specific elements of the methodology that will be included in the assessment. As shown in Figure 2.1, 10 assessment elements are included in the methodology. The appropriateness of each and the level of detail must be examined in the context of the assessment objectives.

As defined below, there are four basic strategies for conducting assessments:

- **Internal.** In-house technical and organizational expertise is used to perform the assessment. In most cases, internal staff members have the distinct advantage of having a clear understanding of the domain, organization, technology, and policies and practices currently in effect. In addition, in-house experts often bring both a historical perspective and a sense of future plans.
- **Facilitated.** In-house technical experts, guided by an outside facilitator, are used to perform the assessment. This option allows a company to offload the organizational and methodological aspects of the assessment to the facilitator and more efficiently leverage internal staff for their specific domain and technical expertise.

- **External.** An external assessment team, such as the OEA national laboratory vulnerability assessment team or a private contractor, conducts the assessment. This approach brings outside objectivity, intra- and inter-industry perspectives, visibility into trends and benchmarks, access to specialized staff with specific expertise, and oftentimes increased credibility with executive management.
- **Hybrid.** Internal staff members perform some elements or tasks, and external experts conduct others.

Because organizations typically do not have the breadth or depth of in-house expertise available to conduct comprehensive vulnerability assessments of the scope defined in Figure 2.1, external expertise is both necessary and desirable. It is also important to note that effective planning, scheduling, coordination, and logistics are as important to completing a successful assessment as assembling a qualified assessment team.

If external expertise is used, well-defined information protection procedures must be established. When the OEA national laboratory team conducts an assessment, a nondisclosure agreement is typically developed that defines the policies for the storage, transmission, handling, and disposition of all sensitive data gathered and generated during the assessment.

## 3.2 CRITICAL ASSET IDENTIFICATION

The final pre-assessment task is to identify and rank critical assets. This is an enterprise-wide ranking of the vital systems, facilities, processes, and information necessary to maintain continuity of service. The objective is to focus the assessment and support the risk analysis process (a process that culminates in ranked options for action). Lists created for Y2K and contingency planning can be a helpful starting point, but a careful analysis of critical assets is needed to ensure that current threats and new critical infrastructure assurance considerations, such as interdependencies, are addressed.

Modern enterprises seek to manage risk in a manner that manages cost while providing adequate protection or mitigation against loss. Delineating the relative importance of corporate assets is necessary for managing risk, but determining their specific importance or criticality is rarely straightforward, particularly in large and complex organizations. The role of critical asset identification within a risk management structure is described. The method (a workshop) of taking the first steps in identifying and categorizing the assets is then described, along with sample results.

### *Role of Critical Asset Identification in Risk Management*

The general objective of critical asset identification is straightforward — to identify and prioritize assets according to how critical they are to the company. The result is used to focus the vulnerability assessment. For example, if a supervisory control and data acquisition (SCADA) system were ranked higher than a particular facility with a network, firewalls, etc., the SCADA system would be assessed (theoretically) before the facility network. Caution must be exercised,

however, to ensure the network does not provide access to the SCADA system, thus elevating it to the same priority.

The results of the critical assets identification task are closely linked to the risk characterization task conducted later in the assessment. The primary difference is that the pre-assessment meeting that accomplishes this is the preliminary act of bringing together representatives from across the enterprise to delineate and prioritize assets for the vulnerability assessment. The risk characterization task focuses on the resulting investment and implementation priorities. It requires information on the criticality (or consequences of loss) for assets so that evaluation of the risk benefits or investment can be ranked. For example, assets with low criticality (e.g., whose disruption would result in low consequences) would not merit substantial investment in protection. Such evaluation requires a sense of the cost associated with the consequences, which can be obtained directly or indirectly by utility staff during the workshop.

It is important to use an approach that evaluates all the important corporate assets against a common (across the enterprise) set of criteria. The result is a uniform enterprise-wide prioritization, rather than a business unit by business unit prioritization. This uniformity avoids the disparity in ranking that frequently develops when each business unit conducts its own prioritization. It also provides uniform treatment to common assets such as communications and information technology (IT) networks services.

Identifying asset criticality is a vital element of assessing and managing risk. A typical security-based risk management process is depicted in Figure 3.1.

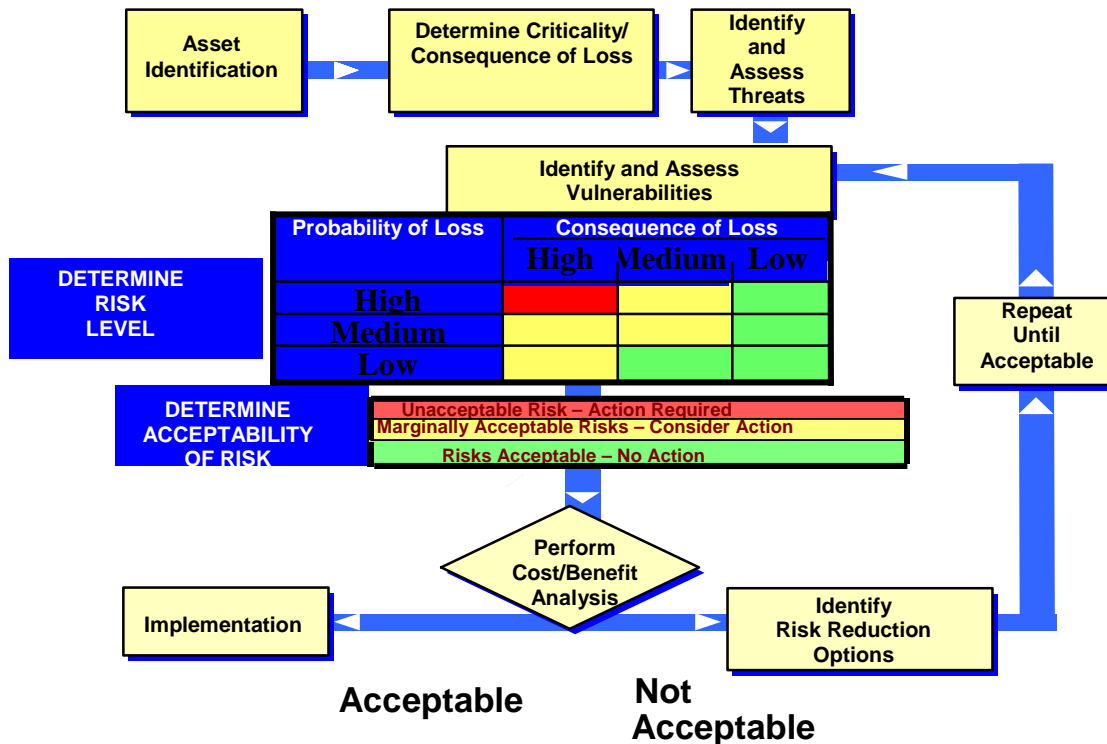


Figure 3.1 Example Risk Management Process (Source: adapted from Federal Aviation Agency, 2000)

Identification of asset criticality serves several functions:

- It enables more careful consideration of factors that affect risk, including threats, vulnerabilities, and consequences of loss or compromise of the asset.
- It enables more focused and thorough consideration of risk mitigation options.
- It enables leaders to develop robust methods for managing consequences of asset loss (restoration).
- It provides a means to increase awareness of a broad range of employees to protect truly critical assets and to differentiate in policies and procedures the heightened protection they require.

As previously indicated, identifying the criticality of assets is used primarily to focus the vulnerability analysis efforts. It also assists with the ranking of the various recommendations for reducing vulnerabilities. Appendix A contains more detailed information on the critical asset methodology, including the critical asset workshop to assist in developing the list of critical assets for the facility.

Potential electric power infrastructure critical assets can include:

#### Physical

- Generators
- Substations
- Transformers
- Transmission lines
- Distribution lines
- Control center
- Warehouses (e.g., equipment, spare parts)
- Office buildings
- Internal and external infrastructure dependencies

#### Cyber

- SCADA system
- Networks
- Databases
- Business systems (e.g., trading, accounting, human resources)
- Telecommunications

#### Interdependencies

- Single-point nodes of failures
- Critical infrastructure components of high reliance

## 4 VULNERABILITY ASSESSMENT METHODOLOGY

As shown in Figure 2.1, the assessment methodology consists of 10 elements. Each element along with its section numbering is listed below.

- 4.1 Network architecture
- 4.2 Threat environment
- 4.3 Penetration testing
- 4.4 Physical security
- 4.5 Physical asset analysis
- 4.6 Operations security
- 4.7 Policies and procedures
- 4.8 Impact analysis
- 4.9 Infrastructure interdependencies
- 4.10 Risk characterization

High-level summaries from each element area are provided below. Appendix B contains the request for information for each element, and Appendix C contains more detailed information on the methodology used for each element, including the approach, process, and tips for each element.

### 4.1 NETWORK ARCHITECTURE

This element provides an analysis of the information assurance features of the information network(s) associated with the organization's critical information systems. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linkage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network.

Procedures for information assurance in the system, including authentication of access and management of access authorization, should be reviewed. The assessment should identify any obvious concerns related to architectural vulnerabilities, as well as operating procedures. Existing security plans should be evaluated, and the results of any prior testing should be analyzed. Results from the network architecture assessment should include potential recommendations for changes in the information architecture, functional areas and categories where testing is needed, and suggestions regarding system design that would enable more effective information and information system protection.

Three techniques are used in conducting the network architecture assessment:

1. Analysis of network and system documentation during and after the site visit;
2. Interviews with facility staff, managers, and Chief Information Officer; and
3. Tours and physical inspections of key facilities.

*(The request for information for network architecture is in Appendix B, Section B.1, and the methodology description is in Appendix C, Section C.1.)*

## **4.2 THREAT ENVIRONMENT**

Development of a clear understanding of the threat environment is a fundamental element of risk management. When combined with an appreciation of the value of the information assets and systems, and the impact of unauthorized access and subsequent malicious activity, an understanding of threats provides a basis for better defining the level of investment needed to prevent such access.

The threat of a terrorist attack to the electric power infrastructure is real and could come from several areas, including physical, cyber, and interdependency. In addition, threats could come from individuals or organizations motivated by financial gain or persons who derive pleasure from such penetration (e.g., recreational hackers, disgruntled employees). Other possible sources of threats are those who want to accomplish extremist goals (e.g., environmental terrorists, antinuclear advocates) or embarrass one or more organizations.

This element should include a characterization of these and other threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterization of the threat environment should be localized, that is, within the organization's service area.

*(The request for information for threat environment is in Appendix B, Section B.2, and the methodology description is in Appendix C, Section C.2.)*

## **4.3 PENETRATION TESTING**

The purpose of network penetration testing is to utilize active scanning and penetration tools to identify vulnerabilities that a determined adversary could easily exploit. Penetration testing can be customized to meet the specific needs and concerns of the utility. In general, penetration testing should include a test plan and details on the rules of engagement (ROE). It should also include a general characterization of the access points to the critical information systems and communication interface connections, modem network connections, access points to principal network routers, and other external connections. Finally, penetration testing should include identified vulnerabilities and, in particular, whether access could be gained to the control network or specific subsystems or devices that have a critical role in assuring continuity of service.

Penetration testing consists of an overall process for establishing the ground rules or ROE for the test; establishing a white cell for continuous communication; developing a format or methodology for the test; conducting the test; and generating a final report that details methods, findings, and recommendations.

Penetration testing methodology consists of three phases: reconnaissance, scenario development, and exploitation. A one-time penetration test can provide the utility with valuable feedback; however, it is far more effective if performed on a regular basis. Repeated testing is recommended because new threats develop continuously, and the networks, computers, and architecture of the utility are likely to change over time.

*(The request for information for penetration testing is in Appendix B, Section B.3, and the methodology description is in Appendix C, Section C.3.)*

#### **4.4 PHYSICAL SECURITY**

The purpose of physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated. Physical security systems include access controls, barriers, locks and keys, badges and passes, intrusion detection devices and associated alarm reporting and display, closed-circuit television (assessment and surveillance), communications equipment (telephone, two-way radio, intercom, cellular), lighting (interior and exterior), power sources (line, battery, generator), inventory control, postings (signs), security system wiring, and protective force. Physical security systems are reviewed for design, installation, operation, maintenance, and testing.

The physical security assessment should focus on those sites directly related to the critical facilities, including information systems and assets required for operation. Typically included are facilities that house critical equipment or information assets or networks dedicated to the operation of electric or gas transmission, storage, or delivery systems. Other facilities can be included on the basis of criteria specified by the organization being assessed. Appropriate levels of physical security are contingent upon the value of company assets, the potential threats to these assets, and the cost associated with protecting the assets. Once the cost of implementing/maintaining physical security programs is known, it can be compared to the value of the company assets, thus providing the necessary information for risk management decisions. The focus of the physical security assessment task is determined by prioritizing the company assets; that is, the most critical assets receive the majority of the assessment activity.

At the start of the assessment, survey personnel should develop a prioritized listing of company assets (see Appendix A). This list should be discussed with company personnel to identify areas of security strengths and weaknesses. During these initial interviews, assessment areas that would provide the most benefit to the company should be identified; once known, they should become the major focus of the assessment activities.

The physical security assessment of each focus area usually consists of the following:

- Physical security program (general)
- Physical security program (planning)
- Barriers
- Access controls/badges
- Locks/keys

- Intrusion detection systems
- Communications equipment
- Protective force/local law enforcement agency

The key to reviewing the above topics is not to just identify if they exist but to determine the appropriate level that is necessary and consistent with the value of the asset being protected. The physical security assessment worksheets provide guidance on appropriate levels of protection.

Once the focus and content of the assessment task have been identified, the approach to conducting the assessment can be either at the “implementation level” or at the “organizational level.” The approach taken depends on the maturity of the security program.

For example, a company with a solid security infrastructure (staffing, plans/procedures, funding) should receive a cursory review of these items; however, facilities where the security programs are being implemented should receive a detailed review. The security staff can act upon deficiencies found at the facilities, once reported.

For companies with an insufficient security organization, the majority of time spent on the assessment should take place at the organizational level to identify the appropriate staffing / funding necessary to implement security programs to protect company assets. Research into specific facility deficiencies should be limited to finding just enough examples to support any staffing / funding recommendations.

*(The request for information for physical security is in Appendix B, Section B.4, and the methodology description is in Appendix C, Section C.4.)*

## **4.5 PHYSICAL ASSET ANALYSIS**

The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist. Included in this element is an examination of asset utilization, system redundancies, and emergency operating procedures. Consideration should also be given to the topology and operating practices for electric and gas transmission, processing, storage, and delivery, looking specifically for those elements that either singly or in concert with other factors provide a high potential for disrupting service. This portion of the assessment determines company and industry trends regarding these physical assets. Historic trends, such as asset utilization, maintenance, new infrastructure investments, spare parts, SCADA linkages, and field personnel are part of the scoping element (see Section 3.1).

The proposed methodology for physical assets is based on a macro-level approach. The analysis can be performed with company data, public data, or both. Some companies might not have readily available data or might be reluctant to share that data.

Key output from analysis should be graphs that show trends. The historic data analysis should be supplemented with on-site interviews and visits. Items to focus on during a site visit include the following:

- Trends in field staffing
- Trends in maintenance expenditures
- Trends in infrastructure investments
- Historic infrastructure outages
- Critical system components and potential system bottlenecks
- Overall system operation controls
- Use and dependency of SCADA systems
- Linkages of operation staff with physical and IT security
- Adequate policies and procedures
- Communications with other regional utilities
- Communications with external infrastructure providers
- Adequate organizational structure

*(The request for information for physical asset analysis is in Appendix B, Section B.5, and the methodology description is in Appendix C, Section C.5.)*

#### **4.6 OPERATIONS SECURITY**

Operations security (OPSEC) is the systematic process of denying potential adversaries (including competitors or their agents) information about capabilities and intentions of the host organization. OPSEC involves identifying, controlling, and protecting generally nonsensitive activities concerning planning and execution of sensitive activities. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and nonsensitive information that might inappropriately aid or abet an individual's or organization's disproportionate influence over system operation (e.g., electric markets, grid operations). This assessment should include a review of security training and awareness programs, discussions with key staff, and tours of appropriate principal facilities. Information that might be available through public access should also be reviewed.

*(The request for information for operations security is in Appendix B, Section B.6, and the methodology description is in Appendix C, Section C.6.)*

#### **4.7 POLICIES AND PROCEDURES**

The policies and procedures by which security is administered (1) provide the basis for identifying and resolving issues; (2) establish the standards of reference for policy implementation; and (3) define and communicate roles, responsibilities, authorities, and accountabilities (R<sup>2</sup>A<sup>2</sup>) for all individuals and organizations that interface with critical systems. They are the backbone for decisions and day-to-day security operations. Security policies and procedures become particularly important at times when multiple parties must interact to effect a desired level of security and when substantial legal ramifications could result from policy violations. Policies and procedures should be reviewed to determine whether they (1) address the key factors affecting security; (2) enable effective compliance, implementation, and

enforcement; (3) reference or conform to established standards; (4) provide clear and comprehensive guidance; and (5) effectively address the R<sup>2</sup>A<sup>2</sup>.

The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of policies and procedures. Understanding and assessing this area provide a means of identifying strengths and areas for improvements that can be achieved through:

- Modification of current policies and procedures
- Implementation of current policies and procedures
- Development and implementation of new policies and procedures
- Assurance of compliance with policies and procedures
- Cancellation of policies and procedures that are no longer relevant, or are inappropriate, for the facility's current strategy and operations

*(The request for information for policies and procedures is in Appendix B, Section B.7, and the methodology description is in Appendix C, Section C.7.)*

#### **4.8 IMPACT ANALYSIS**

A detailed analysis should be conducted to determine the influence that exploitation of unauthorized access to critical facilities or information systems might have on an organization's operations (e.g., market and/or physical operations). In general, such an analysis would require thorough understanding of (1) the applications and their information processing, (2) decisions influenced by this information, (3) independent checks and balances that might exist regarding information upon which decisions are made, (4) factors that might mitigate the impact of unauthorized access, and (5) secondary impacts of such access (e.g., potential destabilization of organizations serving the grid, particularly those affecting reliability or safety). Similarly, the physical chain of events following disruption, including the primary, secondary, and tertiary impacts of disruption, should be examined.

The purpose of the impact analysis is to help estimate the impact that outages could have on a utility. Outages in electric power, natural gas, and oil can have significant financial and external consequences to a utility. The impact analysis provides an introduction to risk characterization by providing quantitative estimates of these impacts so that the utility can implement a risk management program and weigh the risks and costs of various mitigation measures.

*(The request for information for impact analysis is in Appendix B, Section B.8, and the methodology description is in Appendix C, Section C.8.)*

#### **4.9 INFRASTRUCTURE INTERDEPENDENCIES**

The term "infrastructure interdependencies" refers to the physical and electronic (cyber) linkages within and among our nation's critical infrastructures — energy (electric power,

oil, natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. This task identifies the direct infrastructure linkages between and among the infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of an organization's functions, internal infrastructures, and how these link to external infrastructures.

The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.

*(The request for information for infrastructure interdependencies is in Appendix B, Section B.9, and the methodology description is in Appendix C, Section C.9.)*

#### **4.10 RISK CHARACTERIZATION**

Risk characterization provides a framework for prioritizing recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritize the recommendations and assist the organization in determining the appropriate course of action. It provides a framework for assessing vulnerabilities, threats, and potential impacts (determined in the other tasks). In addition, the existing risk analysis and management process at the organization should be reviewed and, if appropriate, utilized for prioritizing recommendations. The degree to which corporate risk management includes security factors is also evaluated.

*(The request for information for risk characterization is in Appendix B, Section B.10, and the methodology description is in Appendix C, Section C.10.)*

## 5 POST-ASSESSMENT

The post-assessment phase involves prioritizing assessment recommendations, developing an action plan, capturing lessons learned and best practices, and conducting training. The risk characterization element results provide the basis for the post-assessment by providing prioritized lists of recommendations that are ranked by key criteria. The company should take the prioritized lists and validate the recommendations and costs. Recommendations that are low cost or result in cost savings should be singled out for special attention. Other recommendations, however, might require formidable financial resources for implementation and require knowledge of the current company financial situation and posture toward risk.

Each company should carefully evaluate the costs and benefits of each recommendation. Recommendations compared in this section include making trade-offs in improvements in each of the other element areas. For example, which physical security measures should be selected versus changes in policies and procedures and network architecture? These are difficult decisions to make and a risk management framework combined with a diverse group of company decision makers should be a part of this decision making process.

The next step is to develop an action plan that includes timelines, staffing assignments, and budgets to implement the proposed recommendations. Lessons learned should be captured along the way to improve the overall process in the future. Training and other technical support activities, such as workshops, are also appropriate throughout the process.

## APPENDIX A: CRITICAL ASSETS METHODOLOGY

### Critical Asset Identification

One approach used to identify critical assets is to conduct a Pre-Assessment Workshop. This is a facilitated workshop involving representatives from a wide diversity of organizational elements. It can provide a cost-effective, one-day session to generate an estimate that is adequate for initiating the assessment process.

The workshop is conducted on the basis of three general steps:

- The definitions and attributes of criticality are reviewed.
- The corporate assets list is generated, based on an intuitive basis of criticality.
- Consensus is reached on the individual assets evaluated and ranked against those attributes.

In addition, a separate listing of special focus areas can be developed. This can provide flexibility for including extraordinary items, that might not otherwise qualify under the criteria, but which are viewed to be sufficiently important to warrant inclusion in the assessment.

It is important that the Pre-Assessment Workshop have representation from all sectors of the enterprise that have or control valuable assets or processes. The representatives should have a reasonable understanding of the operational workings of the company, as well as finance, auditing, risk management, and security. It is not unusual, for example, for the audit group to provide a uniquely balanced perspective of the nontangible assets criticality.

Minimum representation from the following elements is suggested: Corporate Security (or information technology [IT] Security, Physical Security), IT, Administration, Legal, Operations (such as Generation, Transmission, Distribution, Gas Storage, etc.), Audit & Risk Management, Finance, and Human Resources.

**All representatives need to come to the workshop with their organizations' list of critical assets and be prepared to discuss the corporate ranking of the assets.**

### Consequence Basis for Critical Asset Identification

The first step in determining critical assets is to define criticality. Criticality is in the eye of the beholder, and therefore a diverse set of corporate perspectives and knowledge sets must be represented when defining it.

The initial workshop will be the first experience many of the participants will have in this type of endeavor. It is reasonable to expect that some time will be spent instructing the participants in the process and achieving consensus on issues such as the criticality criteria and attributes.

The primary basis for considering criticality is the severity of consequences associated with loss or compromise of the asset. The consequences of asset loss or compromise can have many different dimensions. Therefore, the first portion of the workshop will concentrate on reviewing the determination of those dimensions and associating attributes with different levels of consequences. Three levels of criticality (consequences) may be used for the initial Pre-Assessment Workshop. This is for ease of analysis and documentation, and recognizes that finer resolution may be difficult in an initial exercise of this type. The dimensions of criticality determined are likely to be similar to those of many organizations; however, the attributes that distinguish between various levels of criticality may be unique.

A general guide for developing the criteria for criticality for an energy industry vulnerability assessment might consider the following.

An asset (facility, IT system, node, or network) is considered critical if its destruction, incapacitation, or compromise would:

- Jeopardize the company's long term survival
- Have a serious, harmful effect on the company
- Adversely affect the company's operations or image
- Require near-term, if not immediate remediation

The participants may wish to identify specific, recognizable events or symptoms for each criterion to provide a more clearly defined "trigger." For example, they may define the "high" attribute as, "Would this result in immediate action by the Board of Directors or CEO," and use it as a discriminator to determine critical consequences.

Ranking of recommendations is done in the risk characterization task, but it requires identification of financial consequences of asset loss. For instance, financial losses are defined for each attribute level ranging from a high level (e.g., greater than \$1 billion) to a low level (e.g., less than \$50,000). An approach used in some risk assessments assigns five levels (as opposed to three above) with an appropriate financial consequence associated with each level. Financial consequences of the loss of some assets are difficult to estimate. For these, financial consequences can be assigned because they are valued at a level of similar impact. Hence, the financial consequences can be assumed to be similar. For instance, one might equate the impact of the loss of brand name (which is difficult to assess financially) with the loss of a major facility (whose financial impact is easier to estimate). For evaluating the cost-benefit of mitigating the risks associated with these assets, it would be assumed that they have the same financial consequence if compromised.

It is important to recognize that many of the assets, functions, processes, systems, etc., that are part of a company are very important, but not declared critical. This should not be interpreted as a determination that such assets offer little risk and thus should not be protected. At most, it means that consequences of loss place it lower on the hierarchy for thorough assessment and investment for remediation.

Risks to such assets may still be significant if the threats and vulnerabilities are high. However, many of the measures (e.g., policies and procedures, badging) used to address assets that are more critical also facilitate risk reduction broadly for all assets, including those designated a lower level of criticality. Conversely, an absence of broadly applied security measures, including policies and procedures, increases vulnerability for critical assets for obvious reasons. It also has the indirect effect of increasing vulnerability due to a lack of uniformly educated and alert staff.

Table A.1 provides an example of criticality/consequence dimensions and attributes. The actual dimensions and attributes will vary by company and should be developed by the participants in the workshop. A broad range of attributes should be explored, focusing on attributes that can identify assets that if lost, disrupted, or compromised would have significant consequences.

**Table A.1 Criticality/Consequence Dimensions and Attributes**

Criticality/Consequence Dimensions	Criticality/Consequence Attributes		
	CONSEQUENCE		
Item	High (Board of Directors/CEO)	Medium	Low
<b>Legal Liability</b>			
o Property damage		Mitigated by insurance	Mitigated by insurance
o Health and safety	Multiple loss of life	Loss of life	Minor injury, lost time
o Customer relations	Regional loss of service, >48 hrs	System-wide loss of service	Localized loss of service
o Service interruption	Regional loss of service, long term	Industrial/large commercial outage, safety health (hospital, nursing home)	Small commercial/residential outage
<b>Environmental, Safety and Health</b>			
o Regulatory, environment and safety	Multiple loss of life, major environmental release	Criminal consequence for corp. officer or major negative media event	Minor violation or media exposure
o Employee and labor relations	Property-wide strike and sick-in, service disruption	Property-wide strike	Breach of trust, uncoordinated strike
<b>Financial</b>			
o Shareholder value	Bond rating devaluation to well below investment grade	Bond rating drop of 3 levels, stock devaluation of \$500 million	Bond rating drop of 1 level

Criticality/Consequence Dimensions		Criticality/Consequence Attributes	
	<b>CONSEQUENCE</b>		
Item	High (Board of Directors/CEO)	Medium	Low
o Corporate image		Unexpected executive management exit	Frequent and large billing errors, service deterioration
o Community relations	Alienation of community	Irritation of community	Disgruntled activists
o Competitive impact	Loss of major strategic asset	Loss of medium strategic asset (incl. major class of customers)	Loss of major nonstrategic asset – customers, suppliers
o Business interruption	Executive plane accident	Loss of LAN, telecommunications for 1 month	
o Supply chain impact	Loss of XYZ supply >30 days	Critical equipment failure (replacement issue), transformer, key compressor station or gate station or equivalent failure	
o Political impact	Significant increase in reg. oversight (state or federal)		Significant change in administration (e.g., at Public Utility Commission)
<b>Operations</b>			
o Operations, including unregulated	Total loss of ABC system	Loss of DEF facility	Disruption of operations for 1 week.
o Operations, energy delivery	Simultaneous, coordinated attack on multiassets/ adversary control over SCADA/RTU, loss of all communications	System-wide loss of service, loss of multi-communications	Loss of one major asset
o Operations, generation/production	Simultaneous coordinated loss of multigenerational sites, massive security breach at high-visibility, critical facility	Adversarial control over SCADA/RTU, system-wide loss of service	Loss of one major asset

Critical Asset List

After identifying the criticality dimensions and attributes, the next step in the workshop is to have the attendees list significant assets that might be potentially critical. This includes both information assets (data, applications, networks, systems, processes), as well as physical assets.

After listing the assets, the participants revisit each item and classify it according to criticality. Although the listing from the initial workshop would probably not be exhaustive, it typically would provide a ranking suitable for evaluating major assets for vulnerabilities and provide a ranking of measures for reducing vulnerability and risk.

An example of results comprising an asset listing is provided in Table A.2. It is also important to note which assets have a criticality that depends on the operating or other state of the asset at the time the asset loss occurs. For example, if a number of other assets are out of service, a particular asset could become more critical. In general, these assets rank below those assets with unconditional criticality.

**Table A.2 Critical Asset Listing**

(Assets rated as having High Criticality)

Information Assets	Physical Assets

Special Focus Areas

In addition to critical assets, additional assets or topic areas can be identified that may not fit cleanly within the dimensions and attributes, perhaps because criticality information is not available. Examples might be:

- Remote access from other divisions, supply chain, and other vendors

- Emergency management system vendor access
- Generation vendor access
- “Special” employee modem access
- Relays – access via modem and related laptop data
- Corporate policies regarding access via modem
- Network interconnection (e.g., network to network)

Information to Assist in Determining Critical Assets and Components

- Identify your mission-critical:
  - systems,
  - networks,
  - applications, and
  - data.
- Identify the top five areas of concern that we should focus on and explain why they are important.
- Provide results/reports from any previous testing or analysis.

## APPENDIX B: REQUEST FOR INFORMATION

A preliminary request for information (RFI) is an important part of the vulnerability assessment. The RFI, along with identifying key staff to meet with, is important in the accurate and timely completion of the vulnerability assessment. Some of the RFI sections are quite detailed and may request information that is either not available or cannot be produced in advance of the on-site assessment. In this case, any information that cannot be made available should be noted.

The RFI elements included are:

- B.1 – Network architecture
- B.2 – Threat environment
- B.3 – Penetration testing
- B.4 – Physical security
- B.5 – Physical asset analysis
- B.6 – Operations security
- B.7 – Policies and procedures
- B.8 – Impact analysis
- B.9 – Infrastructure interdependencies
- B.10 – Risk characterization

Each vulnerability assessment element contains information request, personnel to interview, and issues to address. The *information request* provides key information to that specific element so that the analyst can be better prepared for the on-site assessment portion. The *personnel to interview* provides the facility point of contact with an idea of who to line up for interviews, and the *issues to address* gives those individuals a basic idea of potential exploratory areas of questioning.

The information request for some elements may consist of specific information to provide (e.g., maps, diagrams, documents), whereas others may be more like a survey with questions designed to help the analyst better understand the current condition. Note that some staff members are asked to be interviewed for multiple assessment elements.

### B.1 Network Architecture Request for Information

#### Information Request

- Description of the boundaries for this assessment
- Design goals for this implementation (target performance, throughput, reliability, availability target [99.99% uptime?])
- Description of the design process with an emphasis on generation and inclusion of security requirements
- Current network maps (AutoCad Release 13 or earlier, Visio, or PowerPoint format) of infrastructure supporting critical operations systems, business systems, and desktop computing

- Description of authentication mechanisms for local (on-site), Internet, and dial-up access to infrastructure systems
- Description of authorization and access control mechanisms for systems and data
- Description of technical countermeasures (firewall, filtering, proxies, intrusion detection) currently deployed
- Network equipment (routers, switches, firewalls, intrusion detection) vendor, model, and the version/versions of code running on the equipment
- Network protocols in use (e.g., IP, IPX, Appletalk, OSI)
- Routing protocols in use (e.g., RIP, OSPF)
- Maintenance/spares for equipment kept on site
- Methods for scheduling preventive maintenance (down time)
- Methodology for disaster recovery, or fail-over to secondary sites
- Configuration management, both in the core of the network
- Network contact for clarification on infrastructure issues
- Network operational policies
- Network operational procedures
- Network security plans

#### Personnel to Interview

- Chief Information Officer
- Network Security Officer
- Network/Infrastructure designers
- Network administrator(s) to walk through the network maps
- Network administrator(s) to walk through firewall configurations and/or ACLs on routers
- Network administrator/administrators that manage wide area networking

#### Issues to Be Addressed

- Single points of failure
- Known vulnerabilities
- History of failures, break-ins, or break-in attempts

## **B.2 Threat Environment Request for Information**

#### Information Request

- Do employees receive annual security briefings that contain information on potential threats to the employee and to the company? What office is responsible for developing and updating this presentation?
- Does the participant have a relationship with local, state, and federal law enforcement agencies to maintain an understanding of potential threats facing the industry?
  - If yes, what agencies and who are the points of contact for these relationships?
  - Is there an opportunity for the Vulnerability Assessment Program (VAP) to assist participant representatives in establishing contact with local and federal law enforcement agencies to obtain current threat information?

- Does the participant have a history of physical or electronic intrusions? Has a disgruntled/disenchanting employee ever caused, or threatened to cause, property damage? Have any incidents involved the theft of proprietary information?
  - If yes, please provide as much information as possible concerning each incident, including preventive measures taken.

#### Personnel to Interview

- Physical Security Director
- Chief Information Officer
- Human Resources Manager
- City police department representative (crime analyst)
- Local FBI representative (Domestic Terrorism Department)
- Local ATF representative (Domestic Terrorism and Hate Groups Departments)
- US Marshal's representative
- Local Drug Enforcement Agency representative
- Local Secret Service representative
- State Homeland Security representative (intelligence analyst)
- County/Sheriff's representative (crime analyst)
- State/Highway Patrol representative (crime analyst)

#### Issues to Be Addressed

- Historical incidents
- Known threats
- Specific threats to the company
- Threats to the industry other than the specific company
- Methods/techniques commonly used by individuals/groups to cause damage in the community and to gain media attention
- Extreme environmental and animal rights groups in the area and their *modi operandi*
- Known hate groups and their *modi operandi*
- Any known connections between environmentalist/animal rights groups and hate groups
- Presence of possible international terrorist organizations within the community
- Size of the Muslim population within the community and organizations associated with the Muslim community
- Any known connections between the Muslim community/organizations and environmentalist/animal rights groups and hate groups

### **B.3 Penetration Testing Request for Information**

Penetration testing is the only vulnerability assessment element that does not require an RFI. As part of the methodology (described in Appendix C, Section C.3), the tester(s) acquire information through public sources combined with analysis.

## B.4 Physical Security Request for Information

### Information Request

How are the assets/sites/facilities currently being protected?

#### *Security Program*

- Is there a designated security organization? (Give short description)
- What is the level of management support for the security program?
- Has top management established, and effectively disseminated, security policies?
- Is the security policy a part of all managers' responsibilities?
- Are adequate resources (budgetary, staffing) allocated to the security program?
- What is the structure of the security organization within the company? (Attach organizational chart.)
- How many staff members are assigned to the security function?
- How are security staff responsibilities broken out, by functional area (e.g., management, personnel, physical, protective [guard] force, information, operations security)?
- Are policies and procedures documented and in place for the security functional areas (i.e., physical and operations security, review of security policies)?
- Are disciplinary procedures in place?
- Is a security policy in place for handling disgruntled or at-risk employees?
- Is a security policy in place for handling terminated employees?
- Has an executive (senior management) protection plan been developed?
- Has the issue of bomb threats been addressed in policy and communicated to personnel?
- Are telephone "Bomb Threat Checklists" available to personnel?
- Is a self-assessment program in place to evaluate the effectiveness of security programs?
- Are security policies made available to company staff members?
- How are company staff members made aware of security policies?
- Are security staff members provided with adequate training to accomplish their functions?
- Are company staff members provided with initial and refresher security education/awareness training?
- What is the frequency of this training? Are training records (attendance) maintained?
- What does the training consist of (e.g., lecture, computer-based, flyers, posters, hand-out materials)?
- What are the expected responsibilities of management and staff with regard to security?
- How is company property/inventory accounted for (e.g., property tags, periodic inventories, change control) and by whom?
- Is theft/damage of property investigated (and by whom)?
- Is a personnel security (Employment/Human Resources) organization in place to conduct employment screening (background checks/criminal/financial)?

#### *Sites/Facilities*

- What is the layout of the site(s)? (Attach map.)
- Are barriers and postings (no trespassing signs) in place to clearly delineate site boundaries and advise the general public of access restrictions and control points?

- Have the legal aspects and prosecution options been evaluated for trespassing?
- What types of barriers are used at site boundaries (e.g., type [fencing, barricades, alarm zones])?
- Are access control posts staffed and used for entrance to the site?
- What types of entry controls are used for site access (pedestrian/vehicle gates)?
- What types of barriers are used at facility boundaries (i.e., construction materials/walls and doors, windows/bars, one-way film)?
- Do any delineated “security” areas have restricted access (i.e., sensitive storage, computing facilities)?

#### *Access Control*

- What methods of access control are implemented for site access?
- What methods of access control are implemented for facility access?
- Are access control staff (e.g., receptionists) used for controlling access to any sites/facilities?
- Is a lock and key program in place? Who administers this program?
- Are automated access controls (magnetic stripe, proximity card, bar code) used at the sites/facilities? Who administers these systems?
- What is the implementation strategy (policy) for lock and key and/or automated access controls? (How is it determined, and who approves, the specific type of access control device a site/facility will use [i.e., configuration control]?)
- How do personnel request access (i.e., keys, automated access control credentials)?
- Who approves, and how is it determined, who gets access (by key or automated access control credential) to specific areas? Are any checks made before access is granted to an individual?
- How, and where, do personnel obtain their approved keys/automated access control credentials?
- How are keys/automated access control credentials tracked (e.g., entered into a database, paper trail)?
- Are audits conducted of the keys/automated access control programs (i.e., for issued/lost/stolen keys)?
- What happens to an individual’s keys/automated access control credentials when he/she voluntarily leaves employment or is terminated?
- What happens if key/automated access control credentials are determined to be lost or stolen (e.g., locks rekeyed, access removed from automated system)?
- Is a policy in place for delineating under what circumstances locks are to be rekeyed?

#### *Protective Force (PF) (i.e., guards, sentries)*

- Is there a PF dedicated to the site (if so, give the number)?
- What is the command structure of the PF? (Who reports to whom?)
- What are the PF’s protection responsibilities?
- Are the responsibilities delineated in policy and procedures?
- Are PF personnel armed?
- Are PF personnel commissioned (arrest authority, deadly force, credentials)?

- What equipment is issued to PF personnel (vehicles, uniforms, vests, weapons, flashlights)?
- What types of communications equipment are used (two-way radios, telephone, intercom, cellular phone)?
- Is a training program in place for PF personnel?
- What types of training are provided to PF personnel (physical, weapons, assessment)?
- Who certifies and administers the training?
- Are contingency plans in place for incidents that may require PF action?
- Are practice exercises conducted for PF personnel?
- Is an Emergency Preparedness Organization in place?
- Is a Fire Department and/or other hazardous material response capability in place?
- Does the PF coordinate with Emergency Preparedness and Fire Department personnel (including exercises and daily functions)?

#### *Law Enforcement Agency (LEA)*

- Is there a LEA with site protection/incident responsibility?
- If a LEA is the primary response agency, is a Memorandum of Understanding or other form of agreement in place identifying the arrangement?
- What is the LEA's protection responsibility? (What are the expectations of the company?)
- Are the responsibilities delineated in policy and procedures?
- Is a site-specific training program in place for LEA personnel?
- Who administers the training?
- Are contingency plans in place for incidents that may require LEA action?
- Are practice exercises conducted for LEA personnel?
- Does the site coordinate with LEA, Emergency Preparedness, and Fire Department personnel on site (including exercises and daily functions)?

#### *Intrusion Detection/Alarm Systems*

- Are alarm systems used as part of the protection strategy?
- What assets/locations are protected with alarms?
- What types of alarm sensors are used?
- What transmission method is used for alarm systems (hardwire, RF)?
- Is line supervision used for alarm lines?
- Are alarm transmissions encrypted?
- Where are the alarms monitored? Who monitors the alarms?
- What types of alarm monitoring equipment are used?
- How is alarm information reported/displayed?
- Do any alarm systems interface with other emergency systems (e.g., fire detection and suppression, HVAC, water, electric)?
- Are assessment or surveillance devices (CCTV) used?
- Is adequate lighting in place (internal and external) for alarm/intrusion assessment by CCTV and/or human means?

- What power sources (primary and backup) are used for alarm equipment (line, generator, battery/UPS)?
- Is a performance testing/system maintenance program in place for alarm systems?
- Who conducts the testing/maintenance?
- What is the frequency of testing?
- How is maintenance prioritized (e.g., routine, preventive, emergency)?
- How are failed tests handled?
- Are contingency plans in place to address system failures?
- Does the PF/LEA respond to alarms?
- What strategies and authorities are used by the PF/LEA to respond to alarms (delay, interdiction, containment)?

#### Personnel to Interview

- Security Director
- Physical Security Manager
- Facilities Manager
- Contractor Guard Liaison
- Chief Information Officer
- Chief Operations Officer
- Program (i.e., control center) Operations Manager(s)
- Network Security Manager
- Human Resources Manager

#### Issues to Be Addressed

- Security plan/procedures/organization
- Current security strategy
- Changes since 9/11
- Proposed security changes
- Historic/current physical security concerns

### **B.5 Physical Asset Analysis Request for Information**

#### Information Request

- Existing security plan for physical assets
- List of facilities, control centers, etc., where equipment or personnel are stationed
- List of primary assets (including function and location) for electric operations
- System maps showing interconnectivity of assets and components, related capacities, critical customers
- Maintenance procedures and standard practices
- Emergency preparedness plan
- List and location of support equipment, such as maintenance/repair equipment, spare/replacement parts, communications equipment, transportation equipment
- Historic problems that have impacted system operations

- Top (known) threats to safe and continuous operation of electric or gas operations

#### Personnel to Interview

- Chief Operations Officer
- Maintenance Director
- Chief Financial Officer

#### Issues to Be Addressed

- Maintenance practices relative to industry
- Investment strategies toward physical assets/maintenance
- Historic/current problems and concerns

## **B.6 Operations Security Request for Information**

#### Information Request

- Site map
- Simplified facility (facilities) floor plan diagram
- List all information/asset categories that are considered sensitive to the operations/marketing functions of \_\_\_\_\_, in order of relative priority
- Company policy/procedure documentation that would address:
  - Information security (i.e., information protection, storage, marking, transmission, recycling, disposal)
  - Operations security
  - Security training
  - Site badging
  - Requirements for review of information prior to distribution on company Web site
  - Code of Conduct statement

#### *Training*

- What methods are used to distribute company security-related policies to site personnel (e.g., hard copy, e-mail, posters, Web site, staff meetings, computer-based training, group training)?
- Are personnel provided with initial and/or refresher security awareness training?
- Does the security education/awareness program address operations security issues (e.g., information exploitable by adversaries/competitors)?

#### *Personnel Identification*

- Are badges (or other credentials) issued to site personnel?
- Do site personnel wear badges (or other credentials)?
- Is there a visual distinction between types of employee badges (e.g., to provide visual indication that access to some areas is limited)?
- How is visitor/vendor access handled for sites/facilities (e.g., visitor badges, visitor logs, escorts, hosts)?

- Are site personnel encouraged/instructed to challenge individuals who do not display badges?
- Who handles janitorial services (contracted out)?
- What are the janitorial service hours?
- What level of access is granted to janitorial services?

#### *Computing*

- Is any process in place to review the Internet/Intranet information content, for sensitive information, prior to placing it on the Web?
- Who reviews information for release to the public (i.e., is security involved in the review process, as well as communications/public relations/legal)?
- Are periodic reviews conducted of the company's public Web site for operations security concerns (e.g., to determine if sensitive information has inadvertently been placed in the public domain; or if nonsensitive pieces of information could be combined to produce or lead to sensitive information)?
- Is access to the Intranet controlled (e.g., password-protected)?
- Is a policy in place for computer users to use passwords (for network access) and/or password-protected screen savers (for desktop computers)?

#### *Information Handling*

- Is a policy in place for identifying and protecting sensitive information?
- How is computer processing of sensitive information handled (designated locations, use of encryption)?
- How is sensitive information marked (to identify it as sensitive)?
- How is sensitive information protected (when in use, need-to-know policy)?
- How is sensitive information stored (locked rooms, cabinets, security containers)?
- Are special receptacles provided for employees to discard sensitive information?
- Are procedures in place for destruction of sensitive information?
- How is sensitive information destroyed (e.g., shredded, burned, pulped, buried)?
- Who is responsible for the destruction of sensitive information? Is it done internally, or contracted out?
- Are trash receptacles periodically inspected to determine if sensitive information has been improperly thrown out?
- How is sensitive information transmitted and received (encryption)?
- Is there any form of secure fax or phone set up for sensitive facsimile/voice/data transmissions?

#### *Additional Operations Security (Indicators/Awareness Issues)*

- Would any of the following company practices inadvertently provide an adversary or competitor with access to sensitive information or activities of the company?
  - Publishing of certain events, such as schedules, test preparations, routine switches
  - Abrupt changes or cancellations of schedules
  - Purchasing of specialized equipment for sensitive activities (Does purchasing paperwork include information that could identify the sensitivity of the work requiring such equipment?)

- New sensitive facilities/areas (Do these areas telegraph the existence of something special happening?)
- Increased telephone calls, conferences, longer working hours (relating to sensitive upcoming events)
- Exercises to test concepts of operations immediately prior to sensitive upcoming events
- Unusual or increased levels of travel and/or conferences by senior personnel
- “Talking around” sensitive subjects in locations where conversations could be heard by unintended ears
- Discussing personnel, operations, logistics, and communications plans over nonsecure communications (phones, fax, email, radio)
- Company policies and procedures that may reveal sensitive information?
- Distinctive emblems or logos (e.g., markings on uniforms, equipment, or supplies), which may indicate association with sensitive activities?
- Memorandums/advance plans regarding sensitive activities or information
- Access restrictions implemented prior to sensitive activities (telegraphing intentions)
- Overt increases or changes in security operations prior to sensitive activities
- Press releases, company brochures, annual reports concerning general company activities (Do they provide more information than is necessary about staff, company capabilities?)
- Telephone listing with job titles, organizations, and other personnel information identified?

#### Personnel to Interview

- Physical Security Director
- Chief Information Officer
- Chief Operations Officer
- Chief Financial Officer
- Network Security Director
- Human Resources Manager

#### Issues to Be Addressed

- Protecting sensitive information

### **B.7 Policies and Procedures Request for Information**

#### Information Request

- The following policies, procedures, plans, documentation, or the equivalent
  - Technical security and countermeasures
  - Communication (internal and external)
  - Computer security
  - Protected communication
  - Proprietary information
  - Emergency management
  - Physical security

- Operations security
- Human resources (all)
- Contracting
- Training
- Employee manual
- Supervisor/manager manual
- Benefits manual
- Annual report
- Organizational charts
- Emergency management plan
- Code of Conduct or other ethics statements

#### Personnel to Interview

- Security Officer
- Emergency Management Officer
- Corporate Communication Officer
- Public Relations Officer
- Human Resource managers
- Network/System administrators
- Policies/procedures developers/administrators
- Information Security Manager
- Training Manager
- Contracts Officer
- Corporate Attorney
- Several “general population” employees, including bargaining unit employees

#### Issues to be Addressed

- Life-cycle management of policies/plans/procedures
- Policies/plans/procedures in place
- Education/training associated with policies/plans/procedures
- Overall effectiveness of policies/plans/procedures
- Alignment of policies/plans/procedures with corporate objectives and functions

### **B.8 Impact Analysis Request for Information**

#### Information Request

- Historic problems that have affected system operations
- Top (known) threats to safe and continuous operation of electric or gas operations
- Risk management process for including impacts

#### Personnel to Interview

- Chief Financial Officer
- Capital Budgeting Officer

### Issues to Be Addressed

- Current practice of estimating impacts
- Current risk management practices

## **B.9 Infrastructure Interdependencies Request for Information**

### Information Request

- Building diagrams showing internal (i.e., HVAC, fire suppression) infrastructure locations
- Building diagrams showing external (i.e., electric, telecommunications, water, natural gas feeds) infrastructure connections to internal infrastructures and upstream routes (include maps showing routes if available)
- List of facilities and facilities managers
- Emergency and contingency plans
- Risk management activities relating to interdependencies (e.g., investment criteria, risk exposure)
- Y2K plans (or newer contingency plans)
- List of critical infrastructures — electric power, natural gas, oil, telecommunications, transportation (road, rail, air), water, banking and finance, emergency services, and government services — that the utility depends on
  - What function(s) are performed with the commodity/service used?
  - Who are the service providers and points of contact?
  - What types of contracts/service agreements are in place?
- How would the utility be affected by disruptions to the critical infrastructures that serve the utility facilities? What is the severity of such disruptions in terms of the utility operations?
- How do the impacts, and interdependencies concerns, change if the disruptions occur during the workday? During peak load conditions? During Alerts? At night? On a weekend?
- What types of backup systems or other mitigation mechanisms are in place to reduce the impacts to the utility operations from disruptions to supporting infrastructures?
  - What are the limitations of the backup systems as a function of outage duration?
  - How are the backup systems affected by the prolonged outage of other interdependent infrastructures?
  - Does the frequency of disruption affect the backup systems? That is, would repeated disruptions, over several days or weeks, affect infrastructure reliability and response mechanisms? Does it introduce new interdependencies concerns?
- What infrastructure services directly or indirectly impact restoration activities?
- Do dependencies on other infrastructures exacerbate response and recovery efforts?

Personnel to Interview

- Facilities Manager
- Telecommunications Contractor Coordinator
- Critical Systems Manager
- Corporate Services Manager
- Safety and Security Coordinator
- Operations Manager
- Emergency Response Coordinator
- User Support Services Manager
- Director of Financial Planning/Treasurer
- Director of Utility Operations
- Senior Network Analyst
- Human Resources (policies and procedures)
- Lead Strategic Contingency Planner

Issues to Be Addressed

- Single-point infrastructure failures
- Infrastructure backup
- Commercial infrastructure reliance
- Historic/current problems and concerns

**B.10 Risk Characterization Request for Information**Information Request

- Current risk management approach and activities
- Internal and external investment decision criteria

Personnel to Interview

- Chief Financial Officer
- Capital Budgeting Officer
- Physical Security Director
- Chief Information Officer
- Chief Operations Officer
- Network Security Director
- Human Resources Manager

Issues to Be Addressed

- Current risk management approach and activities

## APPENDIX C: VULNERABILITY SURVEY METHODOLOGY

This appendix contains the methodology developed for each of the 10 vulnerability assessment elements listed below:

- C.1 – Network architecture
- C.2 – Threat environment
- C.3 – Penetration testing
- C.4 – Physical security
- C.5 – Physical asset analysis
- C.6 – Operations security
- C.7 – Policies and procedures
- C.8 – Impact analysis
- C.9 – Infrastructure interdependencies
- C.10 – Risk characterization

The description of each element includes information about the approach taken, the process, and tips.

### C.1 Network Architecture Methodology

Three techniques are used in conducting the network architecture assessment:

1. *Analysis* of network and system documentation during and after the site visit;
2. *Interviews* with the facility staff, managers, and Chief Information Officer (CIO); and
3. *Tours* and physical *inspections* of key facilities.

Documentation such as network diagrams, sample system reports, results from previous assessments, and other request for information (RFI) questionnaires (see Appendix B) provided by the facility serve as an introduction to and preliminary background information for the facility's current network architecture. The primary site visit consists of interviews and interaction with facility employees, including technical staff, managers, and the CIO. Questions are asked involving such topics as:

- Network architecture
- Deployed security measures
- Remote access
- Intrusion detection
- Incident response
- Vulnerability assessment activities
- Configuration management
- Cyber security training
- Software development

- Specific questions regarding mission-critical systems such as supervisory control and data acquisition (SCADA)/energy management system (EMS)

The information generated by these discussions provides the core material for the findings and observations. In addition, tours and physical inspections are made at key facilities. During these tours, the network architecture assessment focuses primarily on:

- *Networking equipment* – hubs, switches, routers, firewalls
- *Production equipment* – key servers, workstations
- *Visible connection points* – attached terminals, external modems
- *Physical location of equipment* – wiring closets, raised floors, control rooms, Halon or other fire-protected zones

These inspections provide additional information as well as verification of information previously obtained.

### Network Architecture Tips

Conduct routine system-level security reviews or vulnerability assessments of internal or trusted systems. Supplement outsourced security reviews and vulnerability assessments with frequent, system-level, self-assessment of internal systems across the entire network infrastructure.

- Assure that appropriate external and internal intrusion detection are in place. Intrusion detection (the detection of malicious activities on the network such as unauthorized packet sniffing, port and vulnerability scanning, user access and privilege escalation, or use of common system exploits) is an essential component of any cyber-security program. Facilities should enhance the capability to detect internal malicious activity.
- Consistently implement or screen security measures for remote access, monitoring, and maintenance. Facilities should implement and screen all remote access points.

## **C.2 Threat Environment Methodology**

To address the terrorism threat, the facility should be involved with the ongoing critical infrastructure protection (CIP) activities in the electric power industry. For example, the North American Energy Reliability Council (NERC) has established CIP mechanisms to assist the electric power infrastructure. Through NERC's Critical Infrastructure Protection Advisory Group, physical and cyber security guidelines have been established to better assist companies in matching up appropriate security levels with threat levels. In addition, NERC has established the Indications, Analysis, and Warning Program for sharing incidents with the National Infrastructure Protection Center (NIPC) to trend and monitor potential electric power security issues. The facility should also participate in state Homeland Security activities and other security-related working groups to broaden its depth and understanding of threats. In the absence of established Homeland Security activities or security working groups, the facility should

establish contact with the local FBI office. In addition to providing current threat information relevant to the industry, the FBI can also facilitate the networking of industry to establish security working groups.

The on-site analysis of the threat environment takes place in three phases:

Phase I: An initial screening of sources, prior to the arrival of the vulnerability assessment team, is conducted to identify individual(s) and/or group(s) who are potentially threatening and to establish contact with local, state, and federal law enforcement agencies (LEAs) to begin the analysis process.

Phase II: An on-site assessment is performed, beginning with interviews of facility security managers. The purpose of these interviews is to:

- Determine current corporate security measures (vis-à-vis threats).
- Identify LEAs with whom the *facility* security managers routinely liaison.

Phase III: Office calls are made to federal, state, and local LEAs. The following questions were pursued to determine the threat environment:

- The identities and *modi operandi* of known or suspected individual(s)/group(s) who have initiated hostile actions against any public utilities in the region
- The identities and *modi operandi* of known or suspected individual(s)/group(s) who have threatened hostile action against any public utility in the region
- The identities and *modi operandi* of known or suspected individual(s)/group(s) who have threatened or executed hostile action within the community or its surrounding area to further their “cause”
- The identities and *modi operandi* of known or suspected environmental/animal rights organizations that espouse violent action
- The identities and *modi operandi* of known or suspected “hate groups” (i.e., KKK, White Supremist, Black Panther)
- General assessment of the Muslim population within the community, known or suspected ties to environmental, animal rights, or hate groups, Muslim organizations within the community
- Overall assessment of potential threats to any public utility in the area
- The availability of regularly scheduled LEA intelligence briefings to assist *facility* security personnel
- Points of contacts *facility* security personnel can utilize for questions concerning threats/security
- Incidents and/or threats of any nature by current or former employees of facility
- Assessment of the potential threats to the *facility*

Table C.2.1 contains a list of LEAs that the facility should consider contacting for additional information and/or assistance.

<b>Table C.2.1 List of Organizations to Contact for Threat Information</b>		
<b>Organization</b>	<b>Contact (fill in)</b>	<b>Phone (fill in)</b>
Federal Bureau of Investigation (FBI) Joint Terrorist Task Force (JTTF) - Domestic Terrorism Division		
FBI Field Office		
Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms (ATF) Field Office - Domestic Extremist Section		
ATF Field Office – Intelligence Division		
Department of Justice, U.S. Marshal Service		
City Police Intelligence Division		
NERC		
Other NIPC		
State/Highway Patrol Crime Analyst		
County/Sheriff’s Office Crime Analyst		
Drug Enforcement Agency Crime Analyst (organized crime)		
U.S. Marshal Service		
Department of Justice U.S. Secret Service		
U.S. Customs		
U.S. Border Patrol		
INS		

## Threat Tips

While there may or may not be any known threats that target specific organizations by domestic or international terrorist organizations, continued vigilance is essential. Federal, state, and local LEAs are focused on combating terrorism. Facility security managers need to be proactive in seeking up-to-date threat advisories from LEAs, and all facility personnel should remain vigilant, particularly as more time passes since September 11, 2001. It is important to understand that the increased U.S. security posture will likely not deter terrorist organizations from attacking again and that these organizations are currently in the process of analyzing this nation's security posture to determine weak points. Four threats that the facility should consider include:

Osama Bin Laden's Al-Qaeda and/or other Muslim extremist organizations to strike again in the U.S., as a reprisal for the Coalition's strike against terrorism.

1. Right wing "hate groups" are very active in certain parts of the U.S. Neo-Nazis, Ku Klux Klan, Skinheads, Christian Identity and Neo-Confederates are the main participants in this growing area of domestic terrorism.

Disenchanted employees are very susceptible to coercion and blackmail.

2. Discharged employees are as much of a concern as disenchanted employees.

### C.3 Penetration Testing Methodology

A cyber security penetration test is an effective overall approach for maintaining security. Cyber security must be a continual process of evaluating threats, conducting assessments, and making improvements. The penetration test is a crucial part of the cyber security assessment.

The purpose of a penetration test is to detect potential vulnerabilities of a target network environment and its connected resources using a range of known attack tools and techniques. In contrast to a passive network assessment, a penetration test is an active exercise.

There is great variability in how penetration tests can be conducted, from a minimal port scan to more elaborate methods involving social engineering and firewall penetration. It is important that the customer and the testing agent agree upon what will be done, when it will be done, and what limitations and restrictions will be in effect. This penetration testing methodology addresses these issues as well as discusses the overall process of penetration testing, the importance of establishing a white cell for communications, and basic guidelines for designing and conducting a penetration test. The penetration methodology does not provide the details regarding which attack tools and techniques should be used, as the testing agent would provide that expertise. Rather, the process and steps involved in working with the testing agent to ensure an effective and appropriate testing experience are outlined. By approaching penetration testing as a process, the customer can understand what is being done and feel more in control and confident in the outcome. Potential negative consequences can also be avoided.

The penetration testing process consists of four steps:

1. Defining the rules of engagement (ROE),
2. Establishing a white cell,
3. Designing and conducting the test, and
4. Writing the Final Report.

### Step 1: The Rules of Engagement

The ROE are the basis upon which the penetration test is performed. They are the ground rules for when and how the test will be conducted. Defining the ROE is the first step in the process of working with the testing agent to develop an *authorization list* of what should and should not be done and which networks and systems are eligible for the test. It is important to specify the ROE agreement in detail and then put it in writing. It will then serve as a contract between the customer and the testing agent.

Issues to consider when developing the ROE include:

- Is *a priori* knowledge of the customer's environment available? Will the tester(s) be given any network or system information, or must it be obtained by using reconnaissance techniques?
- When will the test start — day and time?
- What is the duration of the test — one day, multiple days, or ongoing?
- What networks and systems are eligible for testing and which are off limits?
- Are social engineering techniques permitted?
- Are physical penetration attempts and facility surveillance allowed?
- Are port scans of systems and network devices permitted?
- Are penetration attempts of firewall systems allowed?
- How far past the perimeter of the network can the testing agent go?
- How often and when should the testing agent inform the customer of his/her activities and findings?
- Should the testing agent ask permission prior to attempting penetration on a potentially vulnerable system?
- Are home computers of employees off limits? (A potential attack path into a network is from employee computers that dial into or connect via ISP to a remote access gateway on the corporate local area network.)
- Are computers and networks of business partners off limits? (Another potential attack path into a corporate network is via trusted third parties, such as equipment vendors, business partners, and customers that may have direct network connections into the corporate network or otherwise have trusted access through the perimeter via the

Internet.) In general, unless the third parties are informed and consent to a penetration test, this method of testing should not be authorized.

Depending on the comfort level of the customer, more ground rules can be specified to ensure a successful and nondisruptive test. Customers know their environment best and understand what ground rules need to be established. An experienced testing agent will help the customer identify potential issues and provide guidance during the ROE phase of the testing process.

### Step 2: The White Cell

The *White Cell* is the group of people who are aware of when a penetration test is being conducted and what the ground rules are. The white cell consists of the personnel conducting the test and the personnel at the customer's site. It is critical that members of the white cell exchange contact information and maintain communication during the testing period to ensure that the test goes smoothly. One primary reason for establishing a white cell is to avoid a misunderstanding if the network or system administrators detect the test when they have not been informed of the test.

At the very least, the white cell should include a manager who can intercept a detected intrusion attempt and prevent it from escalating within the organization and possibly reported to law enforcement. Customers should decide if they want to inform front-line administrators of the test and include them as members of the white cell. Managers may prefer not to do so in order to see how well existing intrusion detection system (IDS) and security procedures perform in terms of detection and incident handling. If administrators are not included in the white cell, it is imperative to have someone at the customer's site that can intercept a potential incident escalation.

Finally, the white cell should also function as a medium for the tester(s) to continually update the customer on the progress of the test. It should also be used to clarify and resolve potential issues that could occur during the test.

### Step 3: Penetration Test Methodology

As stated earlier, it is not within the scope of this report to discuss the specifics of penetration tools and techniques. Some basic tools are presented as examples; however, it is important for the customer to ask the tester(s) during the ROE establishment phase about the tools and techniques that will be used on the eligible set of systems and networks at the customer's site.

This methodology presents a basic testing format and general guidelines to help customers design a penetration test in consultation with the testing agent. Although the methodology and principles presented here have general applicability to any network environment, attempts will be made to address test design issues specific to the electric utility industry. In particular, a well-designed test for the electric power industry should focus on the mission-critical EMS/SCADA systems that manage the power grid and the market systems that manage the competitive bidding process.

The first consideration in the design of the penetration test is *role simulation*. This type of simulation involves deciding which role the tester(s) will assume during the test. Possible attacker simulation roles are:

1. An Outsider: This is the most common role for penetration testing. The simulated attacker is someone who does not work for the target utility or any other third party that may be associated with the utility, such as a business partner, contractor, vendor, or regulatory agency. The goal of the penetration test is to determine if an outsider with no authorized access to the networks and systems of the utility can subvert the cyber security protections that are in place, such as firewalls, VPN gateways, authentication servers, IDSs, router filters, and access control mechanisms.
2. An Insider: The simulated attacker is someone who works for the utility. There are numerous choices for deciding which internal employee role should be simulated, from an accountant to a technician to a programmer. For utility companies, it may be valuable to provide the tester(s) with access to a typical employee desktop PC to see if they can subvert internal access control protections and reach and possibly subvert mission-critical systems, such as EMS/SCADA systems that manage the power grid.
3. An Associated Third Party: Doing business today means interacting. Modern electric utilities now have network connections to customers, generation facilities, regulators, vendors, and other utilities. While essential for doing business efficiently, these connections also represent potential attack paths into the target utility. By simulating the role of an employee at one of the trusted partner sites, the tester(s) determines if it is possible to penetrate the utility via one of the connections to its trusted business partners.

The most common simulation role for penetration testing is that of the outsider. At a minimum, this role should be simulated in every penetration test so that utilities know if they are vulnerable to cyber attack from the Internet. However, it is increasingly important to consider simulation of the insider and third-party attacker roles. Many security experts contend that most computer crime stems from company staff that have some degree of access to internal systems and networks. Additionally, because many utilities have either dedicated network connections to trusted partners or allow partners to access all or part of their network via the Internet using some form of authentication, it is also useful for the penetration tester(s) to simulate the role of the trusted third party. Arranging this type of test may be more challenging because it requires the willingness and cooperation of the trusted business partner. If the third party will not allow a penetration test to originate from its site, the tester(s) could do a “paper” or analytical assessment of the potential risks involved.

Once the various attacker simulation roles are chosen, a testing format can be devised. An effective testing methodology can be divided into three distinct phases: reconnaissance, scenario development, and exploitation.

1. Reconnaissance: These activities involve gathering information about the target environment in order to plan an attack. The methods used for gathering information

about the target will vary depending on the attack role being simulated, but all will have some techniques in common. During the establishment of the ROE, it is important for the customer and the tester(s) to determine what types of methods are acceptable. For example, social engineering techniques to obtain information may be off limits, whereas searching open information sources (such as a utility Web site, public and regulatory records, articles, employee e-mail and Usenet postings) may be allowable. Another common method used for gathering information for planning an attack is the use of port scanners and other passive probing tools to determine which services are running on a system and additional configuration information about those services.

2. Scenario Development: This phase of the test uses the target information gathered during the reconnaissance phase to develop possible attacks and exploits. After developing the attack scenarios, the tester(s) should present them to the customer. At this point, the customer can decide if some or all of the potential exploits should be tested and what limitation should be applied. It is also an option for the customer to simply accept the scenarios without having the tester(s) demonstrate potential exploits or test the viability of the scenarios. Customers may be content to analyze the information presented and make recommended changes to their environment without the desire for further testing.
3. Exploitation: In this portion of the penetration test, the potential exploits identified in the attack scenarios are carried out. The ROE and scenario discussion with the customer determines which exploits are attempted and which systems and network devices will be targeted. Most customers do not want production servers, network devices, or other mission-critical systems disrupted during the exploitation phase. One way to reduce the possibility of disruption is to prohibit all forms of denial-of-service simulated attacks, which can crash a server or network device. Also the customer can avoid adverse outcomes by identifying (1) noncritical systems for the tester(s) to exploit or (2) an identically configured spare or backup system for the tester(s) to exploit.

The format for the penetration test is as follows. First, the tester(s) conduct reconnaissance, and then based on the target information gathered, develop one or more attack scenarios. At this point, the tester(s) present the scenarios to the customer and explain the potential vulnerabilities involved. The customer then needs to decide which potential exploits should be attempted. Some customers may view the scenarios as hypothetical and will want the tester(s) to carry out the exploits, while other customers will be content to either accept the risk or make security changes to mitigate the risk.

While the test is being conducted, it is critical that the tester(s) maintain constant communication within the white cell, especially during the exploitation phase and to a lesser degree during the reconnaissance phase (since port scanning and social engineering could be involved). During exploitation, the tester(s) should notify the customer of when the exploits are taking place and if any problems occur. Likewise, the customer should be aware of when the controlled attack is occurring and should notify the tester(s) of any problems or disruptions. The white cell team members from the customer site should also be prepared to intercept any incident escalations that

are detected by intrusion detection equipment or by system and network administrators who are not members of the white cell.

The penetration test can be conducted remotely using publicly available network tools, applications, and utilities, such as *ping*, *whois*, *nslookup*, *dig*, *traceroute*, *telnet*, *ftp*, *nmap*, *nessus*, *netcat*, and *whisker*. The penetration test consisted of three primary activities (external reconnaissance, target exploitation, and internal reconnaissance).

### External Reconnaissance

External reconnaissance (“recon”) is conducted by scouting, probing, scanning, and potentially mapping network perimeters that are exposed to the public; mining information from Internet Web sites, newsgroups, e-mails, chat rooms, forums, or other open sources; and ultimately assembling a profile of the target’s strengths and weaknesses. The intent is to discover access points and vulnerabilities that could potentially compromise the target. The following methods can be used against a facility in an attempt to acquire this information:

- **Keyword searches** – keywords, such as *confidential*, *diagram*, *firewall*, *install*, *administrator*, *pin*, *password*, *modem*, *scada*, *download*, *vpn*, *ids*, *intrusion*, *vulnerability*, *https*, and others, can be entered into the company Web site search engine as well as Internet search engines, such as Google, AltaVista, Lycos, and WiseNut.
- **Whois searches** – Internet registry information for the facility can be retrieved from Web-based whois providers, such as the American Registry for Internet Numbers (ARIN) and InterNIC.
- **Company financial research** – The facility’s financial profile or synopsis information can be obtained from financial Web sites, such as <http://finance.yahoo.com>.
- **Connect to common ports** – Some connections to common ports (e.g., Web server port 80, mail server port 25, ftp server port 21) can be made via telnet, Web browser, or other tools to discover accessibility and version information from banners.
- **Traceroute to hosts owned by the facility** – Some traceroutes can be performed for hosts and/or IP addresses associated with the facility. Traceroute information can be used to help determine firewall and general perimeter topology.
- **Resolve IP addresses owned by the facility** – Common tools, such as *nslookup*, *host*, and *dig*, are used to resolve IP addresses associated with the facility.

- **Acquire email message from the facility** – The header of an email message can provide useful information about email routing, internal hosts, and filtering applications such as virus programs.
- **Backwards navigate facility Web sites** – A Web server's directory structure can be traversable by backwards navigating the Web site. For instance, given the URL, <http://www.company.com/projects/docs.html>, a user can probe higher-level directories by iteratively deleting the last subdirectory or file from the URL. For example, by deleting docs.html from the URL and inputting <http://www.company.com/projects/>, the user can see the entire contents of the /projects/ directory. Similarly, by deleting projects/, the user can see the entire contents of the /company/ directory. Note that Web servers can be configured to return the default Web page (e.g., index.html) for that directory or an error message. When the response is a directory listing, backwards navigation is useful for discovering documents, scripts, and other files not necessarily linked to the target Web site.
- **Acquire URLs of scripts or applications from facility Web sites** – Scripts that provide input fields or perform actions on the server can be useful points of entry for a skilled adversary. Scripts often contain bugs that can allow an adversary to manipulate data or compromise a host.
- **Scan IP addresses registered to the facility** – Various scans can be performed using assorted scanners, such as nmap, nessus, and whisker. Scans are used to determine live/responding hosts, open ports, and potential vulnerabilities.

### Target Exploitation

The purpose of this activity is to remotely gain control of or retrieve internal information from vulnerable systems. In general, target exploitation consists of the following:

- **Determine potential targets** –The results from recon are analyzed to determine the most attractive targets.
- **Acquire or develop exploits** – Given the suspected vulnerabilities, exploits or exploit information are acquired and analyzed from open sources, such as [www.securityfocus.com](http://www.securityfocus.com), [www.packetstormsecurity.org](http://www.packetstormsecurity.org), [www.insecure.org](http://www.insecure.org), and the bugtraq newsgroup. Exploits are developed or modified as needed.
- **Execute the exploits** –Exploits against the vulnerable hosts are attempted. Exploits can involve such techniques as automated brute-force password guessing, parameter or command manipulation or injection, taking advantage of misconfigurations or default settings, pushing systems or applications beyond capacity, and subverting intended function or use.

- **Develop Scenarios** –Plausible scenarios are developed that maximize the utility of successful exploits. This step typically involves escalation of access or user privileges, installation of root kits or remote access tools that provide the attacker with more direct control of a system, implementation of backdoors, obfuscation of presence, covering of tracks, and other activities that ensure the complete (and ideally undetected) compromise of a system.

### Internal Reconnaissance

Internal recon is very similar to external recon, except that all activity is based from a compromised host with internal access. This can be in-depth or limited depending on the nature of the compromise, type of host, tools available, location of the host on the network, and the negotiated rules of engagement. In addition to the activities described above for external recon, internal recon can include the following:

- Install additional tools
- Investigate data and files
- Investigate network and system configuration settings
- Locate, obtain, and attempt to crack password files
- Capture and analyze packets generated by or destined to the compromised host
- Capture keystrokes
- Manipulate system or application configurations/settings

### Step 4: Writing the Final Report

The final report prepared by the tester(s) should contain detailed descriptions of the findings during each phase of the test. For the reconnaissance phase, the report should describe what information was obtained about the customer's network and systems and how it was obtained. If port scanning was done, the results of the scans should be made available. For the attack scenario phase, descriptions of the scenarios should be in the report. Likewise, the methods used by the tester(s) during the exploitation phase and the results of the exploits should be described in detail.

Another important element of the report is recommendations. The tester(s) should describe how the vulnerabilities discovered can be fixed or mitigated. Recommendations can range from installing a simple operating system patch on a server to making significant changes and upgrades to the security architecture of the network. If the tester(s) was able to use open-source searching or successfully use social engineering techniques to obtain useful information about the customer's network, the report should recommend how to prevent information from leaking in the future.

## C.4 Physical Security Survey Methodology

### Process/Detailed Approach

The steps for conducting the physical security assessment are:

1. List critical company assets as identified in the “Critical Asset Identification” step of the VAP assessment process (see Appendix A). The list should be prioritized.
2. Discuss with company personnel the strengths and weaknesses of security programs protecting the critical assets. During these initial interviews, identify assessment areas that would provide the most benefit to the company. These should become the major focus of the assessment activities.
3. Review documentation associated with the physical security programs present for the critical assets. Complete the assessment documents, “Criteria Worksheets to Evaluate Physical Security Programs.”
  - a) Criteria worksheets are used to determine the sophistication of the physical security programs that protect company assets. Initially complete the worksheets during documentation reviews. Confirm the information contained in the worksheets during interviews with personnel responsible for the physical security programs.
  - b) If the company appears to have a functioning security organization, a cursory check of company-wide plans/procedures is sufficient. The majority of the assessment time should be spent at the company’s facilities verifying that its plans and procedures are being implemented.
  - c) If the company does not have a functioning security organization, most of the assessment should be spent on identifying the appropriate staffing/funding necessary to implement security programs for the company. The “Criteria Worksheets to Evaluate Physical Security Programs” can be used as a guide for determining which types of security programs are appropriate.
4. Conduct interviews of personnel responsible for the physical security programs present. Verify the information recorded in the assessment document, “Criteria Worksheets to Evaluate Physical Security Programs.”
5. Review documentation associated with the specific physical security elements implemented to protect company assets. Complete the assessment worksheets in “Physical Security Elements Protecting Critical Assets.”
  - a) For companies with an insufficient security infrastructure, research into specific security element deficiencies should be limited to finding just enough examples to support any staffing/funding recommendations.

- b) Comprehensive assessment activities to review physical security elements protecting critical assets should be conducted only for companies with a solid security infrastructure (staffing, plans/procedures, funding). The security staff can take actions to correct deficiencies found at the facilities, once reported.
  - c) The appropriate level of physical security for the company is contingent upon the value of company assets, the potential threats to these assets, and the cost associated with protecting the assets. These relationships must be considered when conducting an assessment of the security elements.
  - d) Generally speaking, low-cost security elements should be in place at critical assets. Examples include locking doors, wearing identification badges, and escorting visitors. These types of security elements improve the security posture without significant cost and also develop a “security state of mind” for employees.
  - e) Consideration of more stringent security elements (access control points, cameras /alarms, guard force) requires a cost-benefit approach. Recommending that a company eliminate a security element because of high cost may place critical assets at unwarranted risk. Recommending implementation of security elements may be expensive, with little improvement of the overall security posture.
  - f) The “Physical Security Elements Protecting Critical Assets” worksheets contain lists of security elements that are generally used to implement different levels of physical security. Equipped with the prioritized list of company assets, and information from interviews, the tester(s) can use the worksheets to review security elements at a facility and make initial judgments as to the appropriate level of physical security. These initial judgments should be discussed with company security personnel and other assessment team members to develop final recommendations.
6. Conduct tours of the critical assets. Verify the information recorded in the assessment worksheets, “Physical Security Elements Protecting Critical Assets.”

### Implications

The purpose of reviewing the physical security program for the company is to identify what level of security is appropriate, as determined through a risk management approach. The review of physical security provides management with information concerning the value of existing security expenditures, possible low-cost improvements, and potential risk reduction with cost-beneficial security upgrades.

### Findings

The first step in developing findings is to define, “What is a finding?” A finding means that the funding spent on physical security is out-of-balance with the value of the company asset being protected.

No/low-cost physical security elements, such as the wearing of badges, locking doors, etc., provide an increased security posture for a company. If they do not exist, a finding should be considered.

Findings that infer increases in security cost must have a strong cost-benefit rationale to support the finding. Without an accurate cost benefit to the company, company management will reject the finding, and the rest of the findings may be viewed as excessive.

The development of findings should occur through two steps. Initially, findings should be identified through the completion of the assessment worksheets. These should be discussed with company personnel to confirm the accuracy of the information.

The second step in formalizing a finding is an open discussion with the assessment team. Many security findings are interrelated across security functional areas. A specific finding may be a symptom of a larger issue. The assessment team discussion validates findings to the point where they can be documented in preparation for inclusion into a final report.

### Remediation

The process used to develop recommendations is similar to the development of findings. Often, the process happens concurrently with the development of findings. When a problem is found, it is common to ask, “How can it be fixed?”

Interviews with company personnel may provide the best recommendations. Their detailed knowledge of company operations is critical to sound recommendation development.

A list of possible solutions should be developed. Are there any “good practices”, benchmarks, or comparisons that might be made? Is it possible to discuss findings with other physical security professionals? Are there solutions that would resolve multiple findings in physical security or across security topical areas?

Cost benefit to the company is critical in the development of recommendations. Initial and annual costs to implement recommendations must be developed. Analysis must show that the security cost is an attractive value to the company because of the protection provided to the critical assets.

A recommendation is formalized during the open discussion with the assessment team. Several recommendations may be combined, or modified, when all assessment topical areas are viewed together. Implementation of one recommendation may eliminate the need for others. The assessment team discussion validates recommendations to the point where they can be documented in preparation for inclusion into a final report.

### Physical Security Tips

1. Physical security programs should be uniform across an organization. Physical security resources should be optimized around critical assets.
2. A protection strategy should be developed to:
  - a) project an image of a hardened security facility to potential intruders,
  - b) detect intrusion,
  - c) delay intrusion,
  - d) assess alarms by the console operator viewing video, and
  - e) respond with armed personnel.

### Physical Security Worksheets

The following worksheets are included to assist in collecting physical security information:

- Physical Security Program (General) – Table C.4.1
- Physical Security Barriers – Table C.4.2
- Physical Security Access Controls/Badges – Table C.4.3
- Physical Security Locks/Keys – Table C.4.4
- Physical Security Intrusion Detection Systems (IDSs) – Table C.4.5
- Physical Security Communications Equipment – Table C.4.6
- Protective Force/Local Law Enforcement Agency – Table C.4.7
- Entrances into Critical Asset Areas – Table C.4.8
- Surfaces Surrounding Critical Asset Areas – Table C.4.9
- Fences Surrounding Critical Assets – Table C.4.10
- Vehicle Gates through Critical Asset Area Fences – Table C.4.11

<b>Table C.4.1 Physical Security Program (General)</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
1. A mission statement establishing the physical security program exists.			
2. An organizational chart, with areas of responsibility, is developed.			
3. Adequate resources (budgetary and staffing) are present for the physical security program.			
4. An executive (senior management) protection plan has been developed.			
5. "Bomb Threat Worksheets" are available to personnel.			
6. Security staff personnel are provided with adequate training to accomplish their functions.			
7. A threat analysis is included in the security program designing process.			
8. Company assets requiring security are defined.			
9. The level of acceptable risk is defined.			
10. Protection strategies are based on results of a documented vulnerability analysis.			
11. Protection strategies are adequately defined in security planning documents.			
12. Intrusion detection systems (IDSs)(alarms/cameras) and physical security elements (barriers/guards) necessary to meet protection goals are documented.			
13. IDSs (alarms/cameras) and physical security elements (barriers/guards) are tested to demonstrate effectiveness.			

<b>Table C.4.2 Physical Security Barriers</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
14. Physical barriers, such as fences, walls, or doors, are used to define the physical boundaries, delay unauthorized access, and direct the flow of personnel and vehicular traffic through designated portals into critical asset areas.			
15. Vehicle barriers are used to preclude, deter, and where necessary, prevent penetration into critical asset areas when such access cannot otherwise be controlled.			
16. Fences are within 2 inches of firm, hard ground. The fence line should be free of holes, gullies, etc., which would aid in traversing the fence.			
17. Physical protection elements are implemented at all locations where storm sewers, drainage swells, and site utilities intersect the fence perimeter.			
18. Fence lines are kept clear of vegetation, trash, equipment, and other objects that could impede observation.			
19. Fence lines are free of objects that would aid in traversing the fence.			
20. Notification signs are posted as required.			
21. Walls that constitute exterior barriers of critical asset areas should extend from the floor to the structural ceiling, unless equivalent means are used.			

<b>Table C.4.3 Physical Security Access Control/Badges</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
22. Measures are in place at automated or attended access control points that ensure the positive control of personnel attempting to access critical asset areas.			
23. Badges are worn at all times, above the waist, on the exterior garment.			
24. Standard security badges are issued to employees who have long-term routine access to company facilities.			
25. Security badges indicate an employee’s area of authorized access.			
26. Badges for visitors are visibly different than employee security badges.			
27. Badges are destroyed in a manner that precludes reconstruction. If destruction is not immediate, used badges are stored in a secure manner until they can be destroyed.			
28. Individuals are provided information concerning security badge requirements.			
29. Temporary badges are utilized for employees whose security badge has been lost, misplaced, forgotten, or stolen.			
30. A company procedure for security badges provides the following information:  Process for requesting security badges Process for approving the issuance of security badges Control of security badge stock Retrieval of security badges from terminated employees Lost or stolen security badges			

<b>Table C.4.4 Physical Security Locks/Keys</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
31. Security keys are protected at the same level as the asset under protection.			
32. An inventory and accountability system for keys is implemented.			
33. Panic hardware or emergency exit mechanisms used on emergency doors present in critical asset areas are operable only from inside the area and meet all applicable life safety codes.			
34. A company procedure for keys provides the following information:  <ul style="list-style-type: none"> <li>Process for requesting keys</li> <li>Process for approving the issuance of keys</li> <li>Control of key stock</li> <li>Retrieval of keys from terminated employees</li> <li>Lost or stolen keys</li> </ul>			

<b>Table C.4.5 Physical Security Intrusion Detection Systems (IDSs)</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
General			
35. Systems are continuously monitored to assess alarms.			
36. Systems are operated and maintained in a manner that ensures that the number of false alarms does not reduce the system’s credibility.			
37. An audible and optional visual alarm signal capable of alerting the protective force and directing them to the location is required when alarm stations do not monitor alarms.			
38. Compensatory measures are employed when systems are not operating.			
39. Records that are kept on actual and/or false nuisance alarms. Records are reviewed and analyzed, and system malfunctions are corrected.			
40. IDSs in adjacent detection zones overlap, thereby preventing gaps in the detection zone.			
41. Dips, obstructions, equipment, etc., do not provide a pathway for an individual to avoid detection.			
42. The detection zone of exterior alarm systems is kept free of snow, ice, grass, weeds, debris, and any other item that degrades IDS effectiveness. When the above action cannot be accomplished in a timely manner, and when degradation of detection capabilities exists, compensatory measures are taken to provide timely detection.			
43. Operator acknowledgment of alarms is straightforward and easily performed.			
44. The alarm control system has the capability to			

<b>Table C.4.5 Physical Security Intrusion Detection Systems (IDSs)</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
call the central alarm station (CAS) operators' attention to an alarm-associated video recorder/monitor.			
45. The quality of pictures from closed-circuit television (CCTV) cameras allows discrimination between human or animal presence in the camera field-of-view.			
46. Video recorders are actuated by alarm signals and operate automatically with response sufficiently rapid enough to record an actual intrusion.			
47. When used as the principal means of alarm assessment and to determine response level, CCTV cameras have tamper-protection and loss-of-video alarm annunciation.			
48. If remote assessment of a perimeter IDS is used, the coverage is complete, with no gaps between zones.			
49. Objects or shadows do not block CCTV camera field-of-view.			
50. Intrusion detection systems are protected from tampering.			
51. Tamper and system problem indicators are provided on the intrusion detection system in the CAS.			
<b>Lighting</b>			
52. Adequate lighting is available for alarm/intrusion assessment by CCTV and/or human means.			
53. Protective lighting is sufficient to permit detection and assessment of intruders.			
54. Lighting does not produce glare in CCTV			

<b>Table C.4.5 Physical Security Intrusion Detection Systems (IDSs)</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
cameras.  Power Sources  Maintenance Program  55. IDSs receive routine preventive maintenance.  56. IDSs are operability-tested routinely to demonstrate effectiveness.  57. IDSs are functionally tested in accordance with established procedures at a frequency that is documented.  58. Compensatory measures are implemented immediately when any part of the IDS is out of service and are continued until maintenance is complete.  59. Personnel who test and maintain the IDS in use have access authorization consistent with the critical asset area being protected.			

<b>Table C.4.6 Physical Security Communications Equipment</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
60. Communications equipment provides for reliable information exchange between protective force personnel.			
61. Alternate communications capabilities are available immediately upon failure of the primary communications system.			
62. Systems remain operable in the event of loss of primary electric power.			
63. Duress systems are available to protective force personnel.			
64. Activation of the duress alarm is accomplished in as unobtrusive a manner as practicable.			
65. Duress alarms do not annunciate at the post initiating the duress alarm.			

<b>Table C.4.7 Protective Force/Local Law Enforcement Agency</b>			
<b>Criteria</b>	<b>Yes</b>	<b>No</b>	<b>Comment</b>
<p>Protective Force</p> <p>66. The number of protective force members on duty is sufficient to accomplish the mission.</p> <p>67. The command structure is defined.</p> <p>68. The protective force mission is defined.</p> <p>69. Protective force policy/procedures exist.</p> <p>70. Emergency response plans exist.</p> <p>71. The protective force has the equipment necessary to complete the mission (vehicles, uniforms, vests, weapons, flashlights, communications equipment).</p> <p>72. The protective force receives initial and continuing training required.</p> <p>73. The protective force conducts drills/exercises.</p> <p>Local Law Enforcement Agency (LLEA)</p> <p>74. If an LEA is the primary response agency, a Memorandum of Understanding or other form of agreement is in place.</p> <p>75. The LLEA's protection responsibility is defined. (What are the expectations of the company/)</p> <p>76. The LEA participates in drills/exercises.</p>			

<b>Table C.4.8 Entrances into Critical Asset Areas</b>			
<b>Entrance name/location/# _____</b>			
<b>Door Construction</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Wood 9 gauge wire mesh Hollow core metal, no lock/hinge protection			
Hollow core metal Tempered glass panel Security glass panel Half height turnstile			
1/2 inch steel plate Aluminum turnstile Steel turnstile Class V or VI vault Dispensable barrier			
<b>Locks</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
No lock, or lock not used			
Door unlocked, attended by personnel when unlocked ID-actuated lock Padlock High-security padlock Keyed cylinder Combination Mechanically coded			
Electronically coded Two-person –rule-lock systems Lock inaccessible from door exterior			
<b>Personnel controlling access (if used)</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Personnel at post No duress, unprotected			
No duress, small arms protected Duress, unprotected			
Duress, small arms protected Protective force on patrol			
<b>Identification Check</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Casual recognition Credential			
Credential and PIN Picture badge Picture badge and PIN			

<b>Table C.4.8 Entrances into Critical Asset Areas</b>			
<b>Entrance name/location/#</b>			
Exchange picture badge Exchange picture badge and PIN			
Retinal scan and PIN Hand geometry and PIN Speech pattern and PIN Signature dynamics and PIN Fingerprint and PIN			
<b>Explosives Detectors</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Animal olfaction Vapor collection Handheld vapor collection Thermal neutron			
<b>Metal Detectors (Handheld or Portal)</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Ferrous materials only Ferrous and solid lead materials Ferrous materials and all forms of lead			
<b>Item Searches</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Cursory			
Rigorous			
<b>Alarms</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Door penetration sensor Vibration Glass breakage Conducting tape Grid mesh Multiple sensors <b>OR</b> Door position monitor Position switch Balanced magnetic switch			

<b>Table C.4.8 Entrances into Critical Asset Areas</b>			
<b>Entrance name/location/#</b>			
<b>Alarms</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Door penetration sensor Vibration Glass breakage Conducting tape Grid mesh Multiple sensors <b>AND</b> Door position monitor Position switch Balanced magnetic switch			
<b>Alarm Assessment</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
No assessment			
Delayed deployment Timely deployment CCTV w/o instant replay			
CCTV w/instant replay Posted protective force w/duress alarm Automatic deployment of protective force /LLEA			

<b>Table C.4.9 Surfaces Surrounding Critical Asset Areas</b>			
<b>Surface name/location/#</b>			
<b>Surface Construction</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Chain link mesh 16 gauge metal Wood studs and sheet rock Wood studs and plywood Windows			
Clay block 8-inch hollow block 8-inch filled block Windows 9 gauge expanded mesh 1/2-inch diameter × 1-1/4-inch quarry screen 1/2-inch diameter bars with 6-inch spacing 3/16-inch × 2-1/2-inch grating			
8-inch filled rebar block 12-inch filled rebar block 2-inch precast concrete tee 4-inch reinforced concrete 8-inch reinforced concrete 12-inch reinforced concrete 24-inch reinforced concrete			

<b>Table C.4.9 Surfaces Surrounding Critical Asset Areas</b>			
<b>Surface name/location/#</b>			
<b>Roof/Ceiling</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
20 gauge metal with insulation 1/2-inch wood roof Interior drop ceilings			
20 gauge metal built up roof Concrete built up roof with T beam Interior drop ceiling does not extend outside critical asset area			
5-1/2-inch concrete roof 8-inch concrete roof 3-foot earth cover 3-foot soil cement earth cover Interior drop ceiling does not extend outside critical asset area			
<b>Window Alarms</b> (Windows that would be accessible by foot or ladder)	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Window penetration sensor Vibration Glass breakage Conducting tape Grid mesh Multiple sensors <b>OR</b> Interior intrusion sensors (to cover windows that are not alarmed) Sonic Capacitance Video motion Infrared Ultrasonic Microwave Multiple noncomplementary sensors Multiple complementary sensors			
<b>Surface Penetration Alarms</b> (The alarms listed are to provide detection upon attempted penetration of any critical asset area boundary surface.)	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>

<b>Table C.4.9 Surfaces Surrounding Critical Asset Areas</b>			
<b>Surface name/location/#</b>			
Interior intrusion sensors			
Sonic			
Capacitance			
Video motion			
Infrared			
Ultrasonic			
Microwave			
Multiple noncomplementary sensors			
Multiple complementary sensors			
<b>OR</b>			
Exterior intrusion sensors			
Seismic buried cable			
Electric field			
Infrared			
Microwave			
Video motion			
Multiple noncomplementary sensors			
Multiple complementary sensors			

<b>Table C.4.9 Surfaces Surrounding Critical Assets</b>			
<b>Surface name/location/# _____</b>			
<b>Alarm Assessment</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Delayed deployment Timely deployment CCTV w/o instant replay			
CCTV w/instant replay Posted protective force w/duress alarm Automatic deployment of protective force /LLEA			

<b>Table C.4.10 Fences Surrounding Critical Assets</b>			
<b>Fence name/location/# _____</b>			
<b>Fence Construction</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
8-foot chain link			
8-foot chain link with outriggers 8- to 12-foot chain link with outriggers Over 12-foot chain link with outriggers			
<b>Signs</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
“No Trespassing” signs posted			
<b>Vehicle Barriers</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Aircraft cable Concrete blocks Guard rails Steel posts Concrete median Concrete median and ditch Crash I beam Train barrier			

<b>Table C.4.10 Fences Surrounding Critical Assets</b>			
<b>Fence name/location/# _____</b>			
<b>Alarms</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Fence sensors Taut wire Vibration Strain Electric field Multiple sensors <b>OR</b> Intrusion sensors Seismic buried cable Electric field Infrared Microwave Video motion			
Multiple noncomplementary sensors Multiple complementary sensors			
<b>Alarm Assessment</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Delayed deployment Timely deployment CCTV w/o instant replay			
CCTV w/instant replay Posted protective force w/duress alarm Automatic deployment of protective force /LLEA			

<b>Table C.4.11 Vehicle Gates through Critical Asset Area Fences</b>			
<b>Gate name/location/# _____</b>			
<b>Gate Construction</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
No gate closure Vehicle bar			
8-foot chain link 8-foot chain link with outriggers 8- to 12-foot chain link with outriggers Over 12-foot chain link with outriggers			
<b>Vehicle Barriers</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Aircraft cable Blocked by vehicle (gate open) Hydraulic wedge			
<b>Locks</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
No lock, or lock not used			
Gate unlocked, attended by personnel when unlocked ID-actuated lock Padlock High-security padlock			

<b>Table C.4.11 Vehicle Gates through Critical Asset Area Fences</b>			
<b>Gate name/location/# _____</b>			
<b>Personnel controlling access through gate (if used)</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Personnel at post No duress, unprotected			
No duress, small arms protected Duress, unprotected			
Duress, small arms protected Protective force on patrol			
<b>Identification Check</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
Casual recognition Credential			
Credential and PIN Picture badge Picture badge and PIN Exchange picture badge Exchange picture badge and PIN			
Retinal scan and PIN Hand geometry and PIN Speech pattern and PIN Signature dynamics and PIN Fingerprint and PIN			
<b>Explosives Detectors</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Animal olfaction Vapor collection Handheld vapor collection Thermal neutron			

<b>Table C.4.11 Vehicle Gates through Critical Asset Area Fences</b>			
<b>Gate name/location/#</b>			
<b>Metal Detectors (Handheld or Portal)</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Ferrous materials only Ferrous and solid lead materials Ferrous materials and all forms of lead			
<b>Item and Vehicle Searches</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Cursory			
Rigorous			
<b>Alarms</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Fence sensors Taut wire Vibration Strain Electric field Multiple sensors <b>OR</b> Intrusion sensors Seismic buried cable Electric field Infrared Microwave Video motion			
Multiple noncomplementary sensors Multiple complementary sensors			

<b>Table C.4.11 Vehicle Gates through Critical Asset Area Fences</b>			
<b>Gate name/location/# _____</b>			
<b>Alarm Assessment</b>	<b>Security Level</b>		
	<b>Low</b>	<b>Moderate</b>	<b>High</b>
None			
Delayed deployment Timely deployment CCTV w/o instant replay			
CCTV w/instant replay Posted protective force w/duress alarm Automatic deployment of protective force /LLEA			

## C.5 Physical Asset Analysis Survey Methodology

The methodology for physical assets analysis is a macro-level approach. Historic trends such as asset utilization, maintenance, new infrastructure investments, spare parts, SCADA linkages, and field personnel are all in scope. The analysis can be performed with company data, public data, or both. Some companies may not have readily available data or may be reluctant to share that information.

Key output from analysis should be graphs showing trends. The historic data analysis should be supplemented with on-site interviews and visits. Items to focus on during site visit include:

- Trends in field staffing
- Trends in maintenance expenditures
- Trends in infrastructure investments
- Historic infrastructure outages
- Critical system components and potential system bottlenecks
- Overall system operation controls
- Use and dependency of SCADA
- Linkages of operation staff with physical and IT security
- Adequate policies and procedures
- Communications with other regional utilities
- Communications with external infrastructure providers
- Adequate organization structure

Publicly available data such as the FERC Form 1 data provide some maintenance numbers that can be used for industry comparisons. Other public and private data sources are also available for trends analysis.

## C.6 Operations Security Survey Methodology

The first stage of an operations security (OPSEC) review is to gather background information about the facility and learn what critical assets require protection. This review is typically performed through a series of interviews with various departments throughout the company and an Internet presence review. Interviews include meeting with select staff members for details concerning company security, everyday business practices, existing security measures, threat awareness, and potential countermeasures. During the on-site visit to conduct these interviews, a review of existing office security is conducted by walking through various office areas. This review helps to assess the everyday handling of sensitive information throughout the facility.

### 1. Review critical asset list:

- Criteria for critical assets and information:
  - critical to success of operation
  - protected by law

- protected by contractual agreement
  - Information assets include:
    - operational data
    - telecommunications information
    - *IT (databases, security software,....)*
      - legal documents
      - *privacy (i.e., payroll)*
    - economic/financial
  - Physical assets could include:
    - major facilities (main, back up, other)
    - computer, control, communications centers
    - hot standby
    - personnel
2. Review threat against critical assets:
- insider (disgruntled employee or in collusion with outside threat)
  - criminal
  - psychotic
  - hacker
  - terrorists
  - extremists
3. Review adversary access to assets via:
- publications
  - Web site
  - mail
  - press interviews
  - telephone and radio communications
  - modems (remote maintenance of SCADA/EMS, computers, copier)
  - trash
  - contact with employees (direct or phone)
  - requests for proposals
  - job vacancy announcements

4. Ensure employees are trained on:

- what is sensitive
- who is the threat against the assets
- what are their responsibilities to protect the asset

Typical OPSEC output includes:

- List of critical assets
- List of critical staff
- List of critical business systems
  - a) List of sensitive business information (e.g., system diagrams, personal information, medical information, salary information, competitive bids, customer information, disaster recovery plans, and security procedures designed to protect critical assets)

#### OPSEC Tips

1. Web sites should be examined for potentially sensitive information that should be taken off. A policy should be developed and procedures reviewed for placement and removal of various types of information on Web sites.

2. The facility should develop procedures and classifications for marking and destroying sensitive materials.

#### Operations Security Survey Worksheet

This section contains checklists for conducting the OPSEC portion of the survey. The checklists included are:

- C.6.1 Human Resources Security Procedures,
- C.6.2 Facility Engineering,
- C.6.3 Facility Operations,
- C.6.4 Administrative Support Organizations,
- C.6.5 Telecommunications and Information Technologies,
- C.6.6 Publicly Released Information, and
- C.6.7 Trash and Waste Handling.

**Checklist C.6.1 Human Resources Security Procedures**

<b>Date:</b> [MONTH XX, 2002]		<b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>			
<b>(a) Responsibilities</b>			
What internal offices or departments are responsible for dealing with security-related personnel issues?			
<b>(b) Background Checks</b>			
What types of background checks are conducted on employees?			
How extensive are the background checks, and do they vary with the sensitivity of the position?			
<b>(c) Insider Threats</b>			
What current conditions in the organization might create a threat from insiders (e.g., low morale, lay-offs, labor disputes)?			
What are the security procedures for handling disgruntled or at-risk employees?			
What are the security procedures for handling employee termination?			
How many employees have been terminated in the last year?			
<b>(d) Disciplinary Procedures</b>			
What are the policies and procedures for handling incidents of security concern?			
What are the policies and procedures for other disciplinary actions?			

**Checklist C.6.1 Human Resources Security Procedures**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>	
<b>(e) Security Training</b>	
Does the organization's initial and periodic security awareness training program include sections on security contacts, critical assets, threats, sensitive information that needs to be protected, reporting suspicious activities, and employee responsibility?	

**Checklist C.6.2 Facility Engineering**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This section covers security issues related to the engineering information related to the facility. Included are such things as the facility design, configuration, and layout; utility service systems; and building floor plans.	
<b>COMMENTS</b>	
<b>(a) Responsibilities</b>	
What internal offices or departments are responsible for facility engineering?	
<b>(b) Facility Engineering Information</b>	
What facility engineering information (e.g., engineering drawings, site maps, utility service lines, floor plans, entry paths into the facility) is considered sensitive?	
What offices or departments have control of this information?	
What other offices or departments are allowed access to this information?	
What external organizations (e.g., fire departments, environmental agencies) have been given access to this information?	
Is any of the facility engineering information publicly available?	
How is sensitive facility engineering information protected?	
What facility engineering information can be accessed via the computer system or network?	
How is the information disposed of when it is no longer needed?	

**Checklist C.6.2 Facility Engineering**

<b>Date: [MONTH XX, 2002]      Facility: [FACILITY]</b>	
This section covers security issues related to the engineering information related to the facility. Included are such things as the facility design, configuration, and layout; utility service systems; and building floor plans.	
<b>COMMENTS</b>	
<b>(c) Public Access to Facility</b>	
Where are tours allowed within the facility? Describe what portions of the facility are open and who is allowed to tour.	
What portion of the facility is open to the public or special interest groups?	
What periodic meetings are held within the facility where outsiders are allowed inside the facility?	

**CHECKLIST C.6.3 FACILITY OPERATIONS**

<b>Date:</b> [MONTH XX, 2002]		<b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>			
<b>(a) Responsibilities</b>			
What internal offices or departments are responsible for facility operations?			
<b>(b) Facility Operations Control</b>			
Is the operation of the facility controlled from a central point (or several central points)? Describe.			
Is there an automated process control system, energy management system, or SCADA system? Is it isolated or is remote access possible?			
What facility operations control and information are on the computer systems? How is it protected? What other internal organizations have access to operations control capabilities and information?			
Can sensitive operations information be gathered through the telecommunications system (e.g., microwave, cell phones, radio, pagers, voicemail, teleconferencing)?			
Is access to the control point(s) limited to operations personnel? If not, who else has access (e.g., maintenance, janitors, vendors), and how is that access controlled?			
<b>(c) Facility Construction, Repair, and Maintenance</b>			
Are construction, repair, and maintenance at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.			

**CHECKLIST C.6.3 FACILITY OPERATIONS**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>	
Are cleaning and building maintenance (e.g., janitorial service) at the facility done by employees, contractors, or both? If contractors are used, describe procedures for screening and monitoring contractor personnel.	

**Checklist C.6.4 Administrative Support Organizations**

<b>Date:</b> [MONTH XX, 2002]		<b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>			
<b>(a) Procurement</b>		Purchasing and procurement activities include generating need (e.g., requisitions or RFPs), selecting suppliers, documenting purchases, providing delivery of items or services, and payments.	
What internal offices or departments are responsible for reviewing procurement activities from a security perspective?			
What is the security review process for RFPs, contracts, and other procurement documents?			
How is the procurement information protected before release? Include documents, files, copiers, facsimiles, and computer files.			
What security-sensitive information is uniquely marked, both on paper and electronically? Describe how.			
How is security-sensitive procurement information destroyed?			
<b>(b) Legal</b>			
What internal offices or departments are responsible for reviewing legal department activities from a security perspective?			
How are legal documents (e.g., patents, environmental impact statements, safety reports, Securities and Exchange Commission filings, Federal Energy Regulatory Commission filings) reviewed for security implications?			
How are these documents protected?			
How are these documents destroyed when no longer needed?			

**Checklist C.6.4 Administrative Support Organizations**

<b>Date:</b> [MONTH XX, 2002]		<b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>			
<b>(c) Budget and Finance</b>			
What internal offices or departments are responsible for reviewing budget and finance activities from a security perspective?			
How are budget and finance documents reviewed for security implications?			
How are these documents protected?			
How are these documents destroyed when no longer needed?			
<b>(d) Marketing</b>			
What internal offices or departments are responsible for reviewing marketing activities from a security perspective?			
How are marketing materials reviewed for security implications?			
How are these documents protected?			
How are these documents destroyed when no longer needed?			
<b>(e) Internal Information</b>			
What are the policies and procedures for handling “Internal Use Documents” (e.g., memos, notes, newsletters)?			
How are these documents protected?			
How are these documents destroyed when no longer needed?			

**Checklist C.6.5 Telecommunications and Information Technology**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers telecommunications and information technologies. Note that this part of the operations security survey must be coordinated with the portions of the interdependencies survey that address the telecommunications and computer equipment.	
<b>COMMENTS</b>	
<b>(a) Telecommunications</b>	
What are the policies and procedures for communications security?	
What particular equipment carries sensitive traffic? Is this equipment restricted to selected users?	
What training is provided concerning security issues while using telecommunications equipment?	
What level of awareness is there concerning telecommunications equipment being operated in reverse as eavesdropping equipment?	
Is voicemail protected by passwords? Have users changed the vendor-supplied passwords? Is there a master password?	
How are FAX machines protected (e.g., logging, stored information, computer connectivity)?	
Is encryption used on any telecommunications circuits?	
Describe all connections to external radio nets, including paging nets.	
<b>(b) Information Technology</b>	
What are the policies and procedures for computing and information technology security?	
What computer architecture information is available to outsiders?	
What encryption is used for internal files and/or information transmission?	

**Checklist C.6.5 Telecommunications and Information Technology**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers telecommunications and information technologies. Note that this part of the operations security survey must coordinated with the portions of the interdependencies survey that address the telecommunications and computer equipment.	
<b>COMMENTS</b>	
Are system administrators trained to recognize “social engineering attacks” designed to obtain passwords and other security information?	
Describe how e-mail is monitored?	

**Checklist C.6.6 Publicly Released Information**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.	
<b>COMMENTS</b>	
<b>(a) Responsibilities</b>	
What internal offices or departments are responsible for reviewing information (from a security perspective) that is to be released to the public?	
<b>(b) General Procedures</b>	
What is the process used to review information before release?	
How is the information protected before release? Include documents, files, copiers, facsimiles, and computer files.	
<b>(c) Report Release</b>	
Who is responsible for reviewing reports released by the organization?	
<b>(d) Press Contacts</b>	
Who is officially designated to interact with the press?	
How are they trained (including training on security issues)? Who trains them?	
<b>(e) Briefings and Presentations</b>	
Describe how briefings and presentations to be given by employees of the organization are reviewed for security issues.	

**Checklist C.6.6 Publicly Released Information**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.	
<b>COMMENTS</b>	
<b>(f) Public Testimony</b>	
Describe how public testimony that is to be given by employees of the organization is reviewed for security issues.	
<b>(g) Internet Information</b>	
Describe the policy for the review of information posted on the organization's Internet site for security issues.	
What is the required review process for information before it is posted on the Web site?	

**Checklist C.6.7 Trash and Waste Handling**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers the handling of trash and waste that may have security implications (e.g., documents records, discarded equipment).	
<b>COMMENTS</b>	
<b>(a) Responsibilities</b>	
What internal offices or departments are responsible for the security of trash and waste?	
Describe established policies for trash and waste handling.	
<b>(b) Trash Handling</b>	
Where is trash accumulated?	
Is the trash accessible to outsiders?	
Who collects the trash?	
Where is the trash taken?	
<b>(c) Paper Waste Handling</b>	
Where is paper waste accumulated?	
Describe the availability and use of shredders throughout the facility.	
What paper waste is accessible to outsiders?	
Who collects the paper waste?	
Where is the paper waste taken? Is it sent for recycling?	
Describe any on-site destruction of paper waste. How it is protected until destroyed?	
<b>(d) Salvage Material Handling</b>	
Does salvage material (e.g., serviceable equipment no longer needed, surplus equipment) potentially contain sensitive information?	
Describe the procedures for inspecting salvage material before release.	

**Checklist C.6.7 Trash and Waste Handling**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
This checklist covers the handling of trash and waste that may have security implications (e.g., documents records, discarded equipment).	
<b>COMMENTS</b>	
<b>(e) Dumpster Control</b>	
Describe how dumpsters (for trash, paper waste, and salvage materials) that are accessible to the public are monitored to prevent “dumpster diving.”	
How are publicly accessible dumpsters sampled for sensitive information?	

**C.7 Policies and Procedures Survey Methodology**

The methodology used for conducting the policy and procedures portion of the vulnerability assessment includes seven steps.

- 1) The company’s “document tree” should be reviewed to understand what policies and procedures are implemented, which are in development/review cycle, and where there might be gaps. Prior to, during, and after the on-site visit, the company’s policies and procedures should be provided to the review person/team. These should include policies and procedures that address numerous topics, for example, security (physical, information), personnel actions (hiring, terminations, voluntary layoffs) functions (badging, purchasing, contracting, travel) communication (internal, external, public relations). This list is not inclusive: each assessment is driven by the unique characteristics of the company participating in the survey.
- 2) Other company documentation should also be reviewed, including the annual report, organization charts, employee and supervisor/manager manuals, and miscellaneous documents such as mission, vision, values statements and business ethic statements.
- 3) Facility’s public Web site and other public sources should be reviewed to gain additional information about the company and better understanding of its organizational structure and affiliations.
- 4) A visit should be made to the company. The purpose of the visit is to observe the impact of the policies and procedures on the conduct of day-to-day business; learn how policies and procedures are implemented; learn how they are managed (life cycle); acquire operational and functional information; verify information gained prior to the visit; and identify where the company’s security posture would benefit from the implementation of

new policies and procedures, as well as the elimination or modification of policies and procedures.

*This information is gathered through interviews with individuals (as shown in Table C.7.1 below) representing several areas of the company. Generally, the individual interviews require 45-60 minutes each. Once an interview schedule is established and the interviewer knows who will be available for the interviews, the interviewer should draft a protocol for the interviews. While the protocols contain similar questions across companies, because each company is unique, the protocols are tailored for the specific company and representative of the subject area being addressed. Each interviewee should be asked whether the interviewer may make follow-up telephone calls to clarify information noted during the interview.*

**Table C.7.1 List of Interview Candidates for Policies and Procedures Element**

Name	Subject Area
	Security Officers
	Emergency Management Officer
	Corporate Communications Officer
	Public Relations Officer
	Human Resource Managers
	Network/System Administrators
	Policies/Procedures Developers/Administrators
	Information Security Manager
	Training Manager
	Contracts Officer
	Corporate Attorney

- 5) In addition to the informational interviews described in Step 5, brief interviews should be conducted with several employees representing the general employee population, including bargaining unit employees. The purpose of these interviews is to gauge awareness of policies and procedures, to understand the employees' impact on work, and to learn about the employees' perceptions of the company's policies and procedures.
- 6) Information gathered during the interviews and the reviews of documentation is calibrated with other assessment team members. This helps to assure a comprehensive assessment of data and benefits the accuracy of the analysis of information.
- 7) After the on-site visit, all of the information collected as part of the policies and procedures task is analyzed, and the results are used to prepare the assessment report.

### Policies and Procedures Tips

- 1) The facility should develop a standardized process for developing, approving, and issuing policies and procedures.
- 2) Employee education and awareness programs should be conducted on an ongoing basis to ensure policy and procedures are understood and followed.

### **C.8 Impact Analysis Survey Methodology**

The impacts that exploitation of unauthorized access to critical facilities or information systems could have depend on, among other factors, the orientation of the observer. For example, from a company point of view, natural gas and electric operations, costs, and revenues could be affected. From the point of view of the company's customers, there may be economic impacts of lost business activity. From the state and national point of view, there may be a reduction of lost production and business activity. To obtain some perspective on these issues, a few very approximate indicators can be developed.

The impacts of electric and gas outages are both direct (the interruption of an activity, function, or service that requires electricity or natural gas) and indirect (the interruption of activities or services). Examples of direct impacts include business shutdowns, food spoilage, damage to electronic data and equipment, and the inability to operate life-support systems in hospitals and homes. Indirect impacts include property losses resulting from arson and looting, overtime payments to police and fire personnel, and potential increases in insurance rates. Direct and indirect impacts are quantifiable in monetary terms (economic impacts); relate to interruption of leisure or occupational impacts (social impacts); or result in organizational, procedural, and other changes in response to outage conditions [1].

Ideally, value is the total unit price that a consumer would pay for electricity or natural gas at a given level of reliability. Thus, value includes an internal (or monetary) component and an external (or nonmonetary) component such as convenience and comfort. In a typical customer's valuation of electric or natural gas service reliability, the customer implicitly assigns a value to the external component. In some cases, the customer explicitly assigns a monetary value to external costs, as demonstrated by purchases of emergency backup equipment to avoid any power interruptions.

The costs due to an interruption in electric or natural gas service vary from one customer to another, depending on many factors. Even customers within the same class may have widely different costs for the same type of outage. In accordance with the individual customer's tolerance for those costs, each may value more reliable service in differing amounts. For example, in one industry, an outage may only imply postponed production, whereas in another industry, loss of power can ruin production or equipment (e.g., computer chip manufacturing).

With the increasing use of computers and communication systems in all economic activities, a blackout affects all sectors. The major consequences include costs associated with the inability of

the computer to perform critical functions, loss of data, and possible damage to the computer and peripheral equipment. Degradation of storage media is a major concern if the room temperature moves too far from the norm. Critical systems usually have backup power sources, although most are not designed for an extended blackout, when the operating environment becomes more of a concern.

Costs of electric or gas interruptions vary significantly by sector. *Industrial* sector costs are more directly measurable in terms of equipment damage, loss of materials, cost of idle resources, and human health and safety effects. For many *commercial* customers, any electric outage of more than a few seconds has a significant cost due to computer problems, equipment jamming, or ruined product. For example, automatic teller machines at banks will be shut down by a power outage. *Residential* customers are very dependent on electricity for a diverse set of activities and natural gas for space and water heating and cooking. Inconvenience, anxiety, anger, and loss of confidence in the company are probably important considerations for the residential sector.

The difficulty in quantifying the external, nonmonetary component of value has led analysts to quantify only the direct, internal, or monetary component of power interruption costs, while continuing to recognize the existence and importance of external costs in defining an appropriate level of system reliability. Numerous estimates have been made of the direct internal costs of electric service interruptions to various customer classes. The major approaches used to establish these costs include:

- Production factor analysis,
- Economic welfare analysis, and
- Empirical analysis of customer surveys.

In addition, the cost of an electric outage can be expressed in different ways, including the total cost, cost per hour, cost per kilowatt-hour, and cost per demand unit (kilowatt) for various durations of outage. In general, electric outage costs have been estimated to range from \$1 to \$10 per kWh, although specific values depend on the type of customer, the condition of the outage, the length of the outage, and other factors [1]. Similar considerations hold for natural gas outages.

The simplest production factor analysis is to divide the gross domestic product (\$8.7 trillion in 1998) by total electrical generation (3.4 trillion kWh in 1998). This calculation yields a value of \$2.5 per kWh, which serves as a rule of thumb for the value of lost electricity on a nationwide basis [2, 3]. The corresponding figure for the State of (state where assessment is performed) is also approximately (insert # ??) per kWh, based on a gross state product in ???? (most current year) of \$?? billion [3], and electricity sales (used rather than generation to account for net imports) totaled (insert # ??) billion kWh [4].

A lower bound on the values can be obtained by just considering the direct revenue impacts on the company. On a company-revenue basis in ???? (most current year), utility had total revenues of (\$?? from income statement) billion, or approximately \$?? (divide by 365) million per day. The company had (\$?? from income statement) billion in electric revenues and sales of (\$?? from income statement) million kWh [5]. This translates into average revenue of (?? Divide) cents per

kWh. (If natural gas, then gas revenues and sales in million dekatherms [a dekatherm is 10 therms, or approximately 1 million BTU or 1,000 cubic feet of gas] are used to compute the average revenue (\$ per dekatherm).

The costs due to the 1977 New York City blackout have been studied extensively. [1] This blackout is one of the most severe electric outages on record in the U.S. The total cost to businesses, government, Consolidated Edison, Westchester County, insurance, public health services, and other public services (e.g., Metropolitan Transportation Authority) was estimated to be \$822 million (1998 dollars), with \$368 million to small businesses from arson and looting. In addition, Consolidated Edison lost \$14 million in revenues from unserved energy.

The unserved energy was estimated to be 84 million kWh. Dividing the total cost of the outage by the unserved energy gives a unit value of approximately \$9.8/kWh. On an hourly basis, the cost of the 1977 New York City outage was approximately \$34 million per hour.

**Table C.8.1 Estimates of Unit Costs of Outages**

Value	Comment	Sources
9.8 \$/kWh	Based on 1977 New York City blackout	[1]
2.5 \$/kWh	1998 national value, based on GDP/(electric generation)	[2,3]
?? \$/kWh	Utility State Product/(electricity sales)	[3,4]
?? \$/kWh	Utility 1999/2000 electric revenue/(electricity sales)	[5]
?? \$/dekatherm	Utility 1999/2000 electric revenue/(gas sales)	[5]
?? \$ million/day	Utility 1999/2000 average revenues per day	[5]

Using utility average daily sales of ?? million kWh per day (electricity) and ?? thousand dekatherms per day (natural gas), crude estimates can be made of the range of values for a 24-hour outage for the electric or gas systems (Table C.8.2). This is well beyond the magnitude and duration of normal outages based on historical data. However, these values are given here to help bound the analysis and to provide some perspective on the level of consequences that could be associated with an attack by a formidable foe. Clearly, exploitation of vulnerabilities that could lead to outages of electricity or natural gas has potentially serious financial consequences.

**Table C.8.2 Estimated Value of a Utility Energy 24-hour Outage**

Type of Outage	Value (\$million per day)	Comment (see Table C.8.1)
Electric	833	Using the New York 1977 blackout data
Electric	??	Using the national and state ?? \$/kWh based on lost production
Electric	??	Using the state ?? \$/kWh based on lost production
Natural gas	??	Using a multiplier of 50 times the company

Type of Outage	Value (\$million per day)	Comment (see Table C.8.1)
		revenue value as for electricity <sup>a</sup>
Company wide	??	Loss of revenues for an average day
Electric	??	Company lost electric revenues based on the average price of ?? \$/kWh
Natural gas	??	Company lost natural gas revenues based on the average price of ?? \$/dekatherm

<sup>a</sup> The ratio of lost production value of a kWh to the lost revenue value of a kWh in a state was approximately 50. To obtain a similar value for the natural gas part of the company, it was assumed that the ratio of lost production value to lost revenue is also 50 for utility natural gas.

### Impact Analysis Tips

- 1) Estimates of potential consequences and their economic implications are critically important in applying risk management principles to options faced by the company.
- 2) Severe outages can lead to degradation of company reputation and loss of business in a competitive marketplace.

## C.9 Infrastructure Interdependencies Survey Methodology

The primary functions at the facility should be identified. Sample functions may include:

- Manage the company and interact with parent and subsidiary companies.
- Maintain and manipulate company data.
- Contact and communicate with suppliers and customers.
- Manage the electric power transmission system.
- Manage the electric power distribution system.

The infrastructures included in this assessment that potentially support these primary functions are:

- Electric power supply and distribution
- Petroleum fuels supply and storage
- Natural gas supply
- Telecommunications
- Transportation
- Water and wastewater
- Emergency services
- Computers and servers
- HVAC systems
- Fire suppression and fire fighting systems
- SCADA system
- Physical security systems

The assessment focused on determining the infrastructures and infrastructure connections important to the facility. Specifically, the assessment focus included:

1. Determining infrastructure linkages to the Facility's functions
2. Determining linkages between these functions and specific facilities or types of facilities
3. Determining infrastructure connections
4. Assessing infrastructure vulnerabilities
5. Identifying possible infrastructure mitigation measures

The assessment is based on personal interviews with key personnel managing the facility's critical functions, facilities, and infrastructures, along with observing infrastructure components and tracing connections. The types of key staff members to be interviewed are:

- General Manager
- Supervisor, Energy Delivery Group
- Manager, Information Technology Group
- Manager, Emergency Management & Communications
- Manager, Asset Management
- Supervisor, Telecommunications Engineering
- Facility Operations & Maintenance

- Supervisor, Information Technology Group, Systems Programming
- Uniformed Sergeant, Security
- Control Systems Support
- Systems Operations
- Manager, Network Services

### Infrastructure Interdependencies Worksheets

The worksheets/checklists included here are:

- C.9.1 Infrastructure Oversight and Procedures
- C.9.2 Electric Power Supply and Distribution
- C.9.3 Petroleum Fuels Supply and Storage
- C.9.4 Natural Gas Supply
- C.9.5 Telecommunications
- C.9.6 Transportation
- C.9.7 Water and Wastewater
- C.9.8 Emergency Services
- C.9.9 Computers and Servers
- C.9.10 HVAC System
- C.9.11 Fire Suppression and Fire Fighting System
- C.9.12 SCADA System
- C.9.13 Physical Security System
- C.9.14 Financial System

A “set” of checklists (C.9.2 through C.9.14) should be completed for the facility as a whole and for each of the critical assets within the facility. It may be that some parts of the checklist for certain infrastructures may refer to the checklist of another infrastructure. For example, if an infrastructure has its own electric power supply and distribution system, that system would be included in the checklist for that infrastructure. However, if the infrastructure depends entirely on the asset’s or facility’s electric power supply and distribution system for its electric power, the checklist for that infrastructure need only reference the appropriate electric power supply and distribution infrastructure checklist. Also, it may be that the checklists for certain infrastructures of some assets may simply refer to the checklist for that infrastructure for the facility as a whole if that infrastructure supports more than one or all of the critical assets.

**Checklist C.9.1 Infrastructure Oversight and Procedures**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]	
<b>COMMENTS</b>	
<b>(a) Infrastructure Oversight</b>	
<p>Does the facility have a central office or department (such as building management, plant services, facility management) that is responsible for overseeing all or most the infrastructures? Indicate the office/department and list the infrastructures for which they have responsibility and the extent of their responsibilities.</p>	
<p>What coordination or oversight role does the physical security office have as to the infrastructures that support critical functions or activities?</p>	
<b>(b) Infrastructure Procedures</b>	
<p>In general, are operating procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, their availability to relevant staff, and the extent to which they are regularly followed. (Note: details about procedures for specific individual infrastructures are addressed in the relevant checklists.)</p>	

**Checklist C.9.1 Infrastructure Oversight and Procedures**

<b>Date: [MONTH XX, 2002]      Facility: [FACILITY]</b>	
<b>COMMENTS</b>	
<p>Are contingency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: contingencies refer to situations brought about by a failure or disruption within an infrastructure or the infrastructures that support it.)</p>	
<p>If they exist, have the contingency procedures been tested, and are they exercised regularly either as a part of normal operations as through specially designed drills? Describe the drills and their results.</p>	
<p>Are emergency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff. (Note: Emergencies refer to situations brought about by external stress on the facility such as high demands.)</p>	
<p>If they exist, have the emergency procedures been tested, and are they exercised regularly through specially designed drills? Describe the drills and their results.</p>	

**Checklist C.9.2 Electric Power Supply and Distribution**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Primary Source of Electric Power</b>
<b>(b) Electric Distribution System</b>
<b>(c) Backup Electric Power Systems</b>
<b>(d) Commercial Electric Power Sources</b>
<b>(e) Commercial Electric Power Pathways</b>
<b>(f) Commercial Electric Power Contracts</b>
<b>(g) Historical Reliability</b>

**Checklist C.9.3 Petroleum Fuels Supply and Storage**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Uses of Petroleum Fuels</b>
<b>(b) Reception Facilities</b>
<b>(c) Supply Contracts</b>

**Checklist C.9.4 Natural Gas Supply**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Sources of Natural Gas</b>
<b>(b) Pathways of Natural Gas</b>
<b>(c) Natural Gas Contracts</b>
<b>(d) Historical Reliability</b>

**Checklist C.9.5 Telecommunications**

<b>Date:</b> [MONTH XX, 2002]	<b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].	
Note: This checklist includes internal communications (voice, FAX, Intranet, data transfer, e-mail), microwave/radio communications, and Internet and commercial communications.	
DESCRIPTION AND COMMENTS	
<b>(a) Internal Telephone System</b>	
<b>(b) Data Transfer</b>	
<b>(c) Cellular/Wireless/Satellite Systems</b>	
<b>(d) Intranet and E-mail System</b>	
<b>(e) Redundant Access to Intranet and E-mail System</b>	
<b>(f) On-site Fixed Components of Microwave/Radio System</b>	
<b>(g) Mobile and Remote Components of Microwave/Radio System</b>	
<b>(h) Commercial Telecommunications Carriers</b>	
<b>(i) Pathways of Commercial Telecommunications Cables</b>	
<b>(j) Historical Reliability of Commercial Carriers</b>	
<b>(k) Backup Communications Systems</b>	

**Checklist C.9.6 Transportation**

<b>Date:</b> [MONTH XX, 2002]	<b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].	
Note: This checklist includes road, rail, air, water, and pipeline.	
<b>DESCRIPTION AND COMMENTS</b>	
<b>(a) Road Access</b>	
<b>(b) Road Access Control</b>	
<b>(c) Rail Access</b>	
<b>(d) Rail Access Control</b>	
<b>(e) Airports and Air Routes</b>	
<b>(f) Waterway Access</b>	
<b>(g) Waterway Access Control</b>	
<b>(h) Pipeline Access</b>	
<b>(i) Pipeline Access Control</b>	

**Checklist C.9.7 Water and Water System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Primary Domestic Water System</b>
<b>(b) Domestic Water Supply</b>
<b>(c) Backup Domestic Water System</b>
<b>(d) Primary Industrial Water System</b>
<b>(e) Industrial Water Supply</b>
<b>(f) Backup Industrial Water System</b>
<b>(g) Primary Industrial Wastewater System</b>
<b>(h) Backup Wastewater System</b>
<b>(i) Commercial/Public Water Supply Reliability</b>
<b>(j) Commercial/Public Wastewater System Reliability</b>

**Checklist C.9.8 Emergency Services**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
Note: This infrastructure area is not of primary concern for this survey and can be eliminated if useful information is not readily available.
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Local Police</b>
<b>(b) County/State Police</b>
<b>(c) Federal Bureau of Investigation (FBI)</b>
<b>(d) Fire Department</b>
<b>(e) Emergency Medical Services</b>

**Checklist C.9.9 Internal Computers and Servers**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
Note: This infrastructure area is not of primary concern for this survey and can be eliminated if useful information is not readily available.
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Electric Power Sources</b>
<b>(b) Environmental Control</b>
<b>(c) Protection</b>

**Checklist C.9.10 HVAC System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
Note: This checklist includes air handlers, heating plants, cooling towers, and chillers.
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Primary HVAC System</b>
<b>(b) Supporting Infrastructure</b>
<b>(c) Backup HVAC Systems</b>

**Checklist C.9.11 Fire Suppression and Fire-Fighting System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Alarms</b>
<b>(b) Fire Suppression</b>
<b>(c) Fire Fighting</b>
<b>(d) Other Systems</b>

**Checklist C.9.12 SCADA System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Type of System</b>
<b>(b) Control Centers</b>
<b>(c) Electric Power Sources</b>
<b>(d) Communications Pathways</b>
<b>(e) Remote Components</b>
<b>(f) Dedicated SCADA Computers and Servers</b>

**Checklist C.9.13 Physical Security System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Electric Power Sources</b>
<b>(b) Communications Pathways</b>
<b>(c) Computer Support</b>

**Checklist C.9.14 Financial System**

<b>Date:</b> [MONTH XX, 2002] <b>Facility:</b> [FACILITY]
This checklist applies to [the entire facility/ASSET].
Note: This infrastructure area (includes monetary transactions) is not of primary concern for this survey and can be eliminated if useful information is not readily available.
<b>DESCRIPTION AND COMMENTS</b>
<b>(a) Electric Power Sources</b>
<b>(b) Communications Pathways</b>
<b>(c) Computer Support</b>

### Checklist Considerations: Interdependencies Survey

This section contains questions related to each of the infrastructure interdependency survey checklists and their subsections. These questions are intended for use by the survey teams during preparations for interviews with facility representatives to help assure that all relevant aspects of the critical infrastructures are considered in the survey.

## **(a) Electric Power Supply and Distribution**

### **Primary Source of Electric Power**

- If the primary source of electric power is a commercial source, are there multiple independent feeds? If so, describe the feeds and their locations.
- If the primary source of electric power is a system operated by the facility or asset, what type of system is it?
- If a facility-operated primary electric generation system is used, what are the fuel or fuels used?
- If petroleum fuel is used, what quantity of fuel is stored on site for the primary electric generation system, and how long it would last under different operating conditions?
- If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

### **Electric Distribution System**

- Are the components of the electric system that are located outside of buildings (such as generators, fuel storage facilities, transformers, transfer switches) protected from vandalism or accidental damage by fences or barriers? If so, describe the type of protection and level of security it provides.
- Are the various sources of electric power and the components of the internal electric distribution systems such that they may be isolated for maintenance or replacement without affecting the critical functions of the asset/facility? If not, describe the limitations.
- Have any single points of failure been identified for the electric power supply and distribution system? If so, list them and describe.

### **Backup Electric Power Systems**

- Are there additional emergency sources of electric supply beyond the primary system (such as multiple independent commercial feeds, backup generators, uninterruptible power supply [UPS])? If there are, describe them.
- If there is a central UPS, does it support all the critical functions of the asset/facility in terms of capacity and connectivity? Specify for how long it can operate on battery power and list any potentially critical functions that are not supported.
- If there is a backup generator system, does it support all the critical functions of the facility in terms of capacity and connectivity? Specify the fuel and list any potentially critical functions that are not supported.
- Is the fuel for the backup generator system a petroleum fuel? If yes, specify the quantity stored on site and how long it would last.
- If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

### **Commercial Electric Power Sources**

- How many substations feed the area of the asset/facility and the asset/facility itself? That is, is the area supplied by multiple substations? If more than one, which ones have sufficient individual capacities to supply the critical needs of the asset/facility?
- How many distinct independent transmission lines supply the substations? Indicate if an individual substation is supplied by more than one transmission line and which substations are supplied by independent transmission lines.

### **Commercial Electric Power Pathways**

- Are the power lines into the area of the asset/facility and into the asset/facility itself aboveground (on utility poles), buried, or a combination of both? If both, indicate locations of portions aboveground.
- Do the power lines from these substations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.
- Are the paths of the power lines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.

- Are the paths of the power lines located in areas susceptible to natural or accidental damage (such as overhead lines near highways; power lines across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.

### **Commercial Electric Power Contracts**

- What type of contract does the asset/facility have with the electric power distribution company or transmission companies? Specify the companies involved and whether there is a direct physical link (distribution or transmission power line) to each company.
- If there is an interruptible contract (even in part), what are the general conditions placed on interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has electrical service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.

### **Historical Reliability**

- Historically, how reliable has commercial electric power been in the area? Quantify in terms of annual number of disruptions and their durations.
- Typically, when power outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify the duration of the outages.
- Have there ever been electric power outages of sufficient frequency and duration so as to affect the critical functions and activities of the asset/facility?

## **(b) Petroleum Fuels Supply and Storage**

### **Uses of Petroleum Fuels**

- Are petroleum fuels used in normal operations at the asset/facility? If yes, specify the types and uses.
- Are petroleum fuels used during contingency or emergency operations such as for backup equipment or repairs? If yes, specify the types of fuels and their uses.

### **Reception Facilities**

- How are the various petroleum fuels normally delivered to the asset/facility? Indicate the delivery mode and normal frequency of shipments for each fuel type.

- Under maximum use-rate conditions, are there sufficient reception facilities (truck racks, rail sidings, surge tank capacity, barge moorings) to keep up with maximum contingency or emergency demand)? If no, explain where the expected shortfalls would be and their impacts.
- Are the petroleum fuel delivery pathways co-located with the rights-of-way of other infrastructures or located in areas susceptible to natural or accidental damage (across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.
- Are contingency procedures in place to allow for alternative modes or routes of delivery? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility.

### **Supply Contracts**

- Are contracts in place for the supply of petroleum fuels? Specify the contractors, the types of contracts, the modes of transport (pipeline, rail car, tank truck), and the frequency of normal shipments.
- Are arrangements for emergency deliveries of petroleum fuels in place? Indicate the basic terms of the contracts in terms of the maximum time to delivery and the minimum and maximum quantity per delivery. Also, indicate if these terms as such that there may be effects on the critical functions and activities of the asset/facility.

## **(c) Natural Gas Supply**

### **Sources of Natural Gas**

- How many city gate stations supply the natural gas distribution system in the area of the asset/facility and the asset/facility itself? If more than one, which ones are critical to maintaining the distribution system?
- How many distinct independent transmission pipelines supply the city gate stations? Indicate if an individual gate station is supplied by more than one transmission pipeline and which stations are supplied by independent transmission pipelines.

### **Pathways of Natural Gas**

- Do the distribution pipelines from the individual city gate stations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.

- Are the paths of the pipelines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.
- Are the paths of the pipelines located in areas susceptible to natural or accidental damage (such as across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.
- Is the local distribution system well integrated (i.e., can gas readily get from any part of the system to any other part of the system)?

### **Natural Gas Contracts**

- Does the asset/facility have a firm delivery contract, an interruptible contract, or a mixed contract with the natural gas distribution company or the transmission companies? Specify the companies involved and whether there is a direct physical link (pipeline) to each company.
- If there is an interruptible contract (even in part), what are the general conditions placed on interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has natural gas service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.
- Does the asset/facility have storage or some other sort of special contracts with natural gas transmission or storage companies? If yes, briefly describe the effect on sustaining a continuous supply of natural gas to the asset/facility.
- In case of a prolonged disruption of natural gas supply, are contingency procedures in place to allow for the use of alternative fuels (such as on-site propane-air, liquefied petroleum gas, or petroleum fuels)? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility.

### **Historical Reliability**

- Historically, how reliable has the natural gas supply been in the area? Quantify by describing any unscheduled or unexpected disruptions. Were there any effects on the critical functions and activities of the asset/facility?
- If operating under an interruptible service agreement, has natural gas service ever been curtailed? If yes, how often, for how long, and were there any effects on the critical functions and activities of the asset/facility?

## **(d) Telecommunications**

### **Internal Telephone System**

- What types of telephone systems are used within the asset/facility? Are there multiple independent telephone systems? Specify the types of systems, their uses, and whether they are copper-wire or fiber-optic based.
- If there are multiple independent telephone systems within the asset/facility, is each one adequate to support the critical functions and activities? Indicate any limitations.
- If there are multiple (from independent systems) or redundant (from built-in backups) switches and cables, are they physically separated and isolated to avoid common causes of failure?
- Are the telephone switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify types of protection provided.

### **Data Transfer**

- For large-volume and high-speed data transfer within the asset/facility, is there a separate system of switches and cables within the asset/facility? Specify the type of systems and whether it is copper-wire or fiber-optic based.
- If there is a separate system for large-volume and high-speed data transfer, are there redundant switches and cables. If yes, describe the situation.
- If there are redundant switches and cables, are they physically separated and isolated to avoid common causes of failure?
- Are the data-transfer switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify the types of protection provided.

### **Cellular/Wireless/Satellite Systems**

- Are cellular/wireless telephones and pagers in widespread use within the asset/facility? If yes, briefly describe their uses.
- If cellular/wireless telephones and pagers are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.
- Are satellite telephones or data links in widespread use within the asset/facility? If yes, briefly describe their uses.
- If satellite telephones or data links are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.

### Intranet and E-mail System

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

### **Redundant Access to Intranet and E-mail System**

- Does the asset/facility have a backup or redundant Intranet and e-mail system? If yes, describe the system and the amount of backup it provides.
- Do areas where critical functions and activities take place have multiple or redundant access to the Intranet and e-mail system?
- If there are multiple access routes, is each one adequate to support the critical functions and activities? If not, specify any limitations.

### **On-site Fixed Components of Microwave/Radio System**

- Are there multiple or redundant radio communications systems in place within the asset/facility? If yes, specify the types of systems and their uses.
- If there are multiple radio communications systems, is more than one system adequate to support all the critical functions and activities of the asset/facility? Specify any limitations.
- Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the radio communications systems? If yes, indicate under what conditions and for how long.
- Do the radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.
- Are the components of the system located outside of buildings (such as antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.

### **Mobile and Remote Components of Microwave/Radio System**

- Are there mobile components to the radio communications system (such as on vehicles or vessels)? If yes, describe the mobile components.
- Are the mobile components of the radio communications system protected from vandalism or accidental damage by locked boxes or lockable vehicle cabs? Specify the types of protection and level of security they provide.
- Are there remote components to the radio communications system (such as relay towers)? If yes, describe them and their uses.
- Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

- Are there environmental controls required for the remote components (such as heating, cooling)? If yes, describe them.
- Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.
- Is physical security provided for the remote components of the radio communications system? If yes, specify the types of security and the level of protection provided.
- Are there alarms at the remote components of the radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and the response procedure.

### **Commercial Telecommunications Carriers**

- Are there multiple telecommunications carriers used by the asset/facility (possibly commercial, contracted, or organization-owned)? List them, specify the service they provide or the type of information carried (such as analog telephone voice and FAX, digital telephone voice, Internet connections, dedicated data transfer), and the type of media used (copper cable, fiber-optic cable, microwave, satellite).

### **Pathways of Commercial Telecommunications Cables**

- Are the telecommunications cables into the area of the asset/facility and into the asset/facility itself aboveground (on utility poles), buried, or a combination of both? If both, indicate locations of portions aboveground.
- Do the telecommunications cables follow independent pathways into the area of the asset/facility and into the asset/facility itself? If not, indicate how independent they are (some common corridors, intersect at one or more points).
- Are the paths of the telecommunications cables co-located with the rights-of-way of other infrastructures? If yes, describe the extent of the co-location and indicate the other infrastructures.
- Are the paths of the telecommunications cables located in areas susceptible to natural or accidental damage (such as overhead cables near highways; cables across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions.
- Do the various telecommunications carriers and cable pathways use separate independent end offices (EO), access tandems (AT), points of presence (POP), and network access points (NAP) to reach the communications transmission backbones? Briefly describe the extent of this independence.

### **Historical Reliability of Commercial Carriers**

- Historically, has the public switched network (PSN) telephone system in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.
- Typically, when telephone outages occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.
- Historically, have the Internet and dedicated data transfer systems in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.
- Typically, when Internet or data transfer connectivity outages or disruptions occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.

### **Backup Communications Systems**

- Are there redundant or backup telephone systems in place if the primary system is disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.
- Are there redundant or backup Internet and dedicated data transfer systems in place if the primary systems are disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.

## **(e) Transportation**

### **Road Access**

- Are there multiple roadways into the area of the asset/facility from the major highways and interstates? Describe the route or routes and indicate any load or throughput limitations with respect to the needs of the asset/facility.
- Are there any chokepoints or potential hazard areas along these roadways such as tunnels, bridges, dams, low-lying fog areas, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.

### **Road Access Control**

- Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by road without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vehicles, and the size or quantity of material that could approach the asset/facility by road.

- Are there uncontrolled parking lots or open areas for parking near the facility where vehicles could park without drawing significant attention? If yes, indicate the number of vehicles and the size or types of vehicles that would begin to be noticed.

### **Rail Access**

- Are there multiple rail routes into the area of the asset/facility from the nearby rail yards or switchyards? Describe the route or routes and indicate any load or throughput limitations with respect the needs of the asset/facility.
- Are there any chokepoints or potential hazard areas along these rail rights-of-way such as tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, rail traffic closures have occurred somewhat regularly.
- Is there sufficient rail siding space at or near the asset/facility to accommodate rail cars if the number of incoming cars exceeds normal expectations or if outgoing cars are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities of the asset/facility would be affected.

### **Rail Access Control**

- Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by rail without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people and rail cars that could approach the asset/facility by rail.
- Are there railroad tracks or sidings near the asset/facility where rail cars could be positioned without drawing significant attention? If yes, indicate the number and the types of rail cars that would begin to be noticed.

### **Airports and Air Routes**

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

### **Waterway Access**

- Are there multiple water routes to the ports, harbors, or landings used by the asset/facility from the open ocean or major waterway? Describe the route or routes and indicate any load, draft, beam, or throughput limitations with respect the needs of the organization.
- Are there any chokepoints or potential hazard areas along these waterways such as bridges, draw or lift bridges, locks and dams, low-lying fog areas, or landslide areas? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.
- Is there sufficient mooring, wharf, or dock space at the ports, harbors, or landings used by the asset/facility to accommodate ships or barges if the number of incoming vessels exceeds normal expectations or if outgoing barges are not picked up as normally scheduled? Indicate the magnitude of this excess capacity in terms of the time period before the critical functions or activities at the asset/facility would be affected.

### **Waterway Access Control**

- Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by water without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vessels, and the size or quantity of material that could approach the asset/facility by water.
- Are there uncontrolled docks or mooring areas near the asset/facility or the ports, harbors, or landings used by the asset/facility where vessels could moor without drawing significant attention? If yes, indicate the number of vessels and the size or types of vessels that would begin to be noticed.

### **Pipeline Access**

- What materials, feedstocks, or products (crude oil, intermediate petroleum products, refined petroleum products, or liquefied petroleum gas [do not include water, wastewater, or natural gas unless there are special circumstances related to these items]) are supplied to or shipped from the asset/facility by way of pipeline transportation?
- Are there multiple pipelines and pipeline routes into the area of the asset/facility from major interstate transportation pipelines? If yes, indicate which pipelines or combinations of pipelines have sufficient capacity to serve the asset/facility.
- List the pipeline owners/operators, indicate the types of service provided (dedicated or scheduled shipments), describe the route or routes, and indicate any capacity limitations with respect the needs of the asset/facility.

- Are there any bottlenecks or potential hazard areas along these pipeline or pipeline routes such as interconnects, terminals, tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, outages or delays have occurred somewhat regularly.

### **Pipeline Access Control**

- Could intruders or others determined to bring down the asset/facility gain access to the pipeline near the asset/facility or elsewhere along the pipeline route? Describe the protective measures that are in place and indicate any pipeline segments or facilities (pump stations, surge tanks) of concern.

## **(f) Water and Wastewater**

### **Primary Domestic Water System**

- Does the asset/facility have a domestic water system? If yes, specify the uses of the water (such as restrooms, locker rooms, kitchens, HVAC makeup water).
- Does the water supply for the domestic water system come from an external source (community, city, or regional water mains) or from an internal system (wells, river, or reservoir)? If internal, describe the system.

### **Domestic Water Supply (external)**

- What type of external water supply system provides the domestic water? Indicate whether it is public or private and its general size (community, city, or regional).
- Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.
- Are the on-site booster water pumps normally dependent on the asset's/facility's primary electric power supply and distribution system?
- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.
- If there is a special UPS, can it support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.
- If there is a special backup generator system, can it support the on-site booster pumps at required levels? Also indicate the type of fuel or fuels used.

- If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it would last.
- If the fuel for the dedicated backup generator for the booster pumps is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

### **Domestic Water Supply (internal)**

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

### **Backup Domestic Water System**

- Is there an independent backup water source to the primary domestic supply system? If yes, specify the type of backup system (wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity fed or requires active pumps (generally electric).
- Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?
- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.
- If there is a special UPS, can it support the backup domestic water source pumps at the required levels? Specify for how long it can operate on battery power.

- If there is a special backup generator system, can it support the backup domestic water source system pumps at the required levels? Also, indicate the type of fuel or fuels used.
- If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### **Primary Industrial Water System**

- Does the asset/facility have an industrial water system? If yes, specify the uses of the water (wash water, process water, generation of process steam, cooling).
- Does the water supply for the industrial water system come from an external source (community, city, regional water mains) or from an internal system (wells, river, reservoir)? If internal, describe the system.

### **Industrial Water Supply (internal)**

- What type of external water supply system provides the industrial water? Indicate whether it is public or private and its general size (community, city, regional).
- Are on-site pumps and/or storage tanks used to boost the pressure or provide for periods of peak usage? If yes, briefly describe them and their purpose.
- Are the on-site booster water pumps for the industrial water system independent of the asset's/facility's primary electric power supply and distribution system?
- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site booster water pumps? If yes, specify them.
- If there is a special UPS, can it support the on-site booster pumps at required levels? Specify for how long it can operate on battery power.
- If there is a special backup generator system, can it support the on-site booster pumps at required levels? Also, indicate the type of fuel or fuels.
- If the fuel for the dedicated backup generator system for the booster pumps is a petroleum fuel, indicate the quantity stored on site and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### **Industrial Water Supply (external)**

- Indicate the source of the water (wells, river, reservoir), the adequacy of the supply's capacity, and whether it is gravity fed or requires active pumps (generally electric).

- Are the on-site industrial water system pumps independent of the asset's/facility's primary electric power supply and distribution system?
- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial water system pumps? If yes, specify them.
- If there is a special UPS, can it support the on-site industrial water system pumps at required levels? Specify for how long it can operate on battery power.
- If there is a special backup generator system, can it support the on-site industrial water system pumps at the required levels? Also, indicate the type of fuel or fuels.
- If the fuel for the dedicated backup generator system for the on-site industrial water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### **Backup Industrial Water System**

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

### **Primary Industrial Wastewater System**

- Does the asset/facility have an on-site industrial wastewater system? If yes, specify the types of wastewater that are processed and the processes used.

- Are the on-site industrial wastewater lift pumps independent of the asset's/facility's primary electric power supply and distribution system?
- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial wastewater lift pumps? If yes, specify them.
- If there is a special UPS, can it support the on-site industrial wastewater lift pumps at required levels? Specify for how long it can operate on battery power.
- If there is a special backup generator system, can it support the on-site industrial wastewater lift pumps at the required levels? Also, indicate the type of fuel or fuels.
- If petroleum fuel is used for the dedicated backup generator system for the on-site industrial wastewater lift pumps, indicate the quantity stored on site and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### **Backup Wastewater System**

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

### **Commercial/Public Water Supply Reliability**

- Historically, has the city water supply in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the supply pressure or flow rate.
- Typically, when disruptions in the city water supply occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.

### **Commercial/Public Wastewater System Reliability**

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

## **(g) Emergency Services (Police, Fire, Emergency Medical)**

### **Local Police**

- How are the local police involved in protecting the asset/facility?
- What are typical response times and response capabilities?
- Have local police provided services in the past? Has their response been helpful?

### **County/State Police**

- How are the county/state police involved in protecting the asset/facility?
- What are typical response times and response capabilities?
- Have county/state police provided services in the past? Has their response been helpful?

### **Federal Bureau of Investigation (FBI)**

- How is the FBI involved in protecting the asset/facility?
- What are typical response times and response capabilities?

- Has the FBI provided services in the past? Has their response been helpful?

### **Fire Department**

- How is the local fire department involved in protecting the asset/facility?
- Do the local fire department provide inspection and/or certification services?
- What are their typical response times and response capabilities?
- Have they provided services in the past? Has their response been helpful?

### **Emergency Medical Services**

- How is the local emergency medical or ambulance service involved in protecting/treating the personnel at the asset/facility?
- Do they provide inspection and/or certification services?
- What are their typical response times and response capabilities?
- Have they provided services in the past? Has their response been helpful?

## **(h) Computers and Servers (Mainframes, Firewalls, Router Equipment)**

### **Electric Power Sources**

- Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the computers and servers? If yes, indicate under what conditions and for how long.
- Do the computers and servers have their own backup electric power supply (local UPSs, generators)? If yes, specify the types of backup and how long they can operate.

### **Environmental Control**

- Does the asset's/facility's central HVAC system provide environmental control to the computer and server areas, or do the computer and server areas have their own independent environmental control system? If they have their own system, specify the type.
- Can the computers and servers operate with a loss of all environmental control? If yes, specify for how long and under what conditions.

- Are there any backup environmental controls explicitly for the computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.

### **Protection**

- Is there special physical security provided for the computer and server areas? If yes, specify the type of security and the level of protection provided.
- Is there special fire suppression equipment (Halon, Inergen, inert gases, or carbon dioxide) in the computer and server areas? If yes, specify the type.
- Are there special features or equipment in the computer and server areas to limit flooding or water intrusion? If yes, describe them.
- Are there alarms for the computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.

## **(i) HVAC System (Air Handlers, Heating Plants, Cooling Towers, Chillers)**

### **Primary HVAC System**

- Can critical functions and activities that depend on environmental conditions continue without the HVAC system? If yes, specify which functions and for how long they can continue under various external weather conditions.
- Is the HVAC system that supplies the areas of the asset/facility where critical functions that depend on environmental conditions are carried out separate from or separable from the general asset/facility-wide HVAC system?

### **Supporting Infrastructures**

- Does the HVAC system (or critical portion thereof) depend on the primary electric power supply and distribution system to supply electric power? Specify under what conditions and for how long.
- Besides or in addition to electric power, what fuel or fuels does the HVAC system (or critical portion thereof) depend on?
- If the HVAC system (or critical portion thereof) depends on natural gas, are there provisions for alternative fuels during a natural gas outage? Specify the fuel and how long the HVAC system can operate on it.

- If the HVAC system (or critical portion thereof) depends on petroleum fuels for adequate operation, specify the type of fuel and how long the HVAC system can operate on the fuel available on site.
- If the HVAC system (or critical portion thereof) depends on petroleum fuels, are arrangements and contracts in place for resupply and management of the fuel?
- Does the HVAC system (or critical portion thereof) depend on water? If it does, specify if the water need is continuous or for make-up purposes only and the quantities/rates involved.
- If the HVAC system (or critical portion thereof) depends on water, is a backup supply in place such as well and pump, storage tank, or tank trucks? Specify how long the HVAC can operate on the backup water supply system.

### **Backup HVAC Systems**

- Is there a separate backup to the HVAC system? If yes, describe the system and the energy and water supply systems it requires.
- Are there contingency procedures in place to continue with the critical functions and activities that take place at the asset/facility during an HVAC outage? If yes, briefly describe them.
- How long can the critical functions and activities at the asset/facility continue using the backup HVAC system or under the contingency procedures?

## **(j) Fire Suppression and Fire Fighting System**

### **Alarms**

- Does the entire asset/facility (or at least most of it) have a fire and/or smoke detection and alarm system? If yes, specify the type of system, how it is monitored, and the response procedure.

### **Fire Suppression**

- Does the entire asset/facility (or at least most of it) have a fire suppression system such as an overhead sprinkler system? If yes, specify the medium (usually water) and whether it is of the flooded-pipe or pre-armed type.
- Does the water supply for the fire suppression system come from city water mains or an on-site system (wells, rivers, reservoir)?

- If the water supply for the fire suppression system comes from city water mains, specify whether there are separate city fire mains and if the pipe from the main to the asset/facility is separate from the domestic water supply.
- If the water supply for the fire suppression system comes from an on-site system, specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity fed or requires active pumps (generally electric).

### **Fire Fighting**

- Does the asset/facility have its own fire-fighting department? If yes, describe it in terms of adequacy to protect the asset/facility.
- Are city or community fire-fighting services available to the facility? If yes, indicate the type of service and the estimated response time.
- Does the water supply for the fire-fighting hydrants come from city water mains? If yes, specify the number of hydrants and indicate their coverage and accessibility.
- If the water supply for the fire hydrants comes from an on-site system (wells, rivers, reservoir), specify the source, indicate the adequacy of the supply's capacity, and indicate if it is gravity fed or requires active pumps (generally electric). Also, specify the number of hydrants and indicate their coverage and accessibility.

### **Other Systems**

- Is there special fire suppression equipment (Halon, Inergen, inert gases, carbon dioxide) in certain areas such as computer or telecommunications areas? If yes, indicate the types and adequacies of these special systems.

## **(k) SCADA System**

### **Type of System**

- Does the asset/facility make use of a substantial SCADA system (i.e., one that covers a large area or a large number of components and functions)? If yes, indicate what functions are monitored and/or controlled, the type of system, and the extent of the system.
- Is the SCADA system independent of the asset's/facility's primary electric power supply and distribution system?
- Is the SCADA system independent of the asset's/facility's telephone system?
- Is the SCADA system independent of the asset's/facility's microwave or radio communications system?

- Is the SCADA system independent of the asset's/facility's computers and servers?

### **Control Centers**

- Where is the primary control center for the SCADA system located?
- Is there a backup control center? If yes, where is it located? Is it sufficiently remote from the primary control center to avoid common causes of failure (fires, explosions, other large threats)?
- Are there backups to the SCADA computers and servers at the backup control center or at some other location? If yes, indicate the location of the backup computers and servers, whether they are completely redundant or cover only the most critical functions, and whether they are active "hot" standbys or have to be activated and initialized when needed.

Note: *The following sets of questions on electric power sources and communications pathways apply to the control centers as well as the other components of the SCADA system.*

### **Electric Power Sources**

- Are there multiple sources of electric supply (multiple independent commercial feeds, backup generators, UPSs) explicitly for the SCADA system? If yes, indicate the types.
- If there is a special UPS, does it support all the functions of the SCADA system in terms of capacity? Specify for how long it can operate on battery power.
- If there is a special backup generator system, does it support all the functions of the SCADA system in terms of capacity?
- What is the fuel or fuels used by the special SCADA backup generator system? If stored on site, specify the quantity stored and how long it would last.
- If the SCADA backup generator fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?

### **Communications Pathways**

- Are there dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system? If yes, specify whether copper-wire or fiber-optic based.

- If there are dedicated multiple independent telephone systems or dedicated switches and cables supporting the SCADA system, is each one individually adequate to support the entire system? Specify any limitations.
- Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.
- Are the dedicated SCADA telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.
- Are there dedicated multiple or redundant radio communications systems in place to support the SCADA system? If yes, indicate the types.
- If there are multiple radio communications systems, is each one individually adequate to support the entire SCADA system? If not, specify any limitations.
- Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the special SCADA radio communications systems? If yes, specify under what conditions and for how long.
- Do the special SCADA radio communications systems have their own backup electric power supply? If yes, specify the type and how long it can operate.
- Are the components of the special SCADA radio communications system (antennae, on-site towers) located outside of buildings protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security provided.

### **Remote Components**

- Are there remote components to the special SCADA radio communications system (such as relay towers)? If yes, identify the components and their locations.
- Are there backup sources of electric power for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.
- Are there environmental controls required for the remote components (heating, cooling) of the special SCADA radio communications system? If yes, describe them.
- Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.

- Is physical security provided for the remote components of the special SCADA radio communications system? If yes, specify the types of security and the level of protection provided.
- Are there alarms at the remote components of the special SCADA radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and loss of fuel reserves? If yes, specify the types of alarms, how they are monitored, and the response procedure.

### **Dedicated SCADA Computers and Servers**

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

## **(I) Physical Security System**

### **Electric Power Sources**

- Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the asset's/facility's primary electric power supply and distribution system the primary electric power source?)?
- Are there multiple sources of electric power for the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the monitoring and alarm systems. Specify what electric power sources are in place.
- If there is a special UPS, can it support all the functions of the monitoring and alarm systems in terms of capacity? Specify for how long it can operate on battery power.
- If there is a special generator system, can it support all the functions of monitoring and alarm systems in terms of capacity? Also, indicate the type of fuel or fuels used.
- If the fuel for the special security generator system is a petroleum fuel, indicate the quantity stored on site and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### **Communications Pathways**

- Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's telephone system?
- Are there multiple independent telephone systems or dedicated switches and cables supporting the monitoring and alarm systems? This could consist of the asset's/facility's telephone system and its backup or redundant systems or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber-optic –cable based.
- Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.
- Are the dedicated monitoring and alarm systems telephone switches and data-transfer switches located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.
- Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's microwave or radio communications system?

- Are there multiple independent microwave or radio communications systems supporting the monitoring and alarm systems? This could consist of the asset's/facility's primary microwave or radio communications system and its backup or redundant systems or combinations of multiple independent radios, antennae, and relay towers. Specify the type of radio systems used.
- Are there multiple sources of electric power for the microwave or radio communications systems dedicated to support the monitoring and alarm systems? This could consist of the asset's/facility's electric power supply and distribution system and its backup or redundant systems or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the special microwave or radio communications systems. If yes, specify the types and how long they can operate.
- Are the components of the special radio communications system dedicated to the monitoring and alarm systems located outside of buildings (antennae, on-site towers) protected from vandalism or accidental damage by fences or barriers? If protected, specify the types of protection and level of security they provide.
- Are there remote components to the special radio communications system dedicated to the monitoring and alarm systems (e.g., relay towers)? If yes, identify the components and their locations.
- Are there backup sources of electric power for the remote components? If used, indicate the type of backup, the fuels used, and the expected length of operations.
- Are there environmental controls required for the remote components of the special monitoring and alarm radio communications system (heating, cooling)? If yes, describe them.
- Are there backup environmental controls for the remote components? If yes, indicate the type of backup, the fuel or fuels used, and the expected length of operations.

### **Computer Support**

- Are the asset's/facility's monitoring and alarm systems normally dependent on the facility's main computers and servers?
- Are there multiple independent computers supporting the monitoring and alarm systems? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems or combinations of multiple independent computers. Specify the type of computers used.

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

#### **(m) Financial System (including monetary transactions)**

##### **Electric Power Sources**

- Are the asset's/facility's financial systems and functions normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the facility's electric power supply and distribution system the primary electric power source?)?
- Are there multiple sources of electric power for the financial systems and functions? This could consist of the facility's electric power supply and distribution system and its backup or redundant systems or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions? Specify what electric power sources are in place.
- If there is a special UPS, can it support all the financial systems and functions? Specify how long it can operate on battery power.
- If there is a special generator system, can it support all the financial systems and functions? Also, indicate the type of fuel or fuels used.
- Is the fuel for the special security generator system a petroleum fuel? Specify the quantity stored and how long it would last. Are arrangements and contracts in place for resupply and management of the fuel?

### Communications Pathways

- Are the asset's/facility's financial systems and functions normally dependent on the asset's/facility's telephone system?
- Are there multiple independent telephone systems or dedicated switches and cables supporting the financial systems and functions? This could consist of the facility's telephone system and its backup or redundant systems or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber-optic cable based.
- Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.
- Are the dedicated telephone switches and data-transfer switches that support the financial systems and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.

### Computer Support

- Are the asset's/facility's financial systems and functions normally dependent on the facility's main computers and servers?
- Are there multiple independent computers supporting the financial systems and functions? This could consist of the facility's main computers and servers and their backup or redundant systems or combinations of multiple independent computers. Specify the type of computers used.
- Are there multiple sources of electrical supply for any computers dedicated to support the financial systems and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions. If yes, specify the type and how long they can operate.
- Does the asset's/facility's central HVAC system provide environmental control for any separate, dedicated computers that support the financial systems and functions?
- How long can the separate, dedicated computers that support the financial systems and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.
- Do the separate, dedicated computers that support the financial systems and functions have their own independent environmental control system? If so, specify the type.

- Are there any backup environmental controls explicitly for the dedicated computers that support the financial systems and functions? If yes, indicate the type of backup and the expected maximum duration of operation.

## C.10 Risk Characterization Survey Methodology

For the risk characterization task, the first step is to develop a list of important characteristics (sometimes called attributes or criteria) to assist in comparing recommendations. Measurement scales are developed to indicate different levels of achievement with respect to the various characteristics. Examples of characteristics include cost to implement the recommendation (both implementation and operating costs) and the level of potential consequences that could result from exploitation of a specific vulnerability.

The next step in the risk characterization task is for members of the assessment team to identify various risk reduction recommendations. The team members rated their own recommendations against the set of characteristics.

The characteristics used in this evaluation are as follows:

1. **Implementation cost** (includes one-time costs, such as equipment cost, labor cost to install, and changes to existing structures) and **implementation time** (in weeks). Obviously, cost is an important characteristic, and the time to implement may be an important consideration for some recommendations.
2. **Change in operating cost** associated with implementing each recommendation (includes maintenance cost, consumables, and staff time to monitor or supervise). If the recommendation resulted in substituting for some procedure or activity, the cost savings associated with the substitution is considered as well as the operating cost of the recommendation. For example, replacing incandescent light bulbs with fluorescent light bulbs would show an operating cost reduction because, for the same lighting requirement, fluorescents use less electricity. (Note: The cost of the bulbs would be the implementation cost.). This characteristic is another component of the total cost for a recommendation.
3. **Attractiveness of asset.** The attractiveness of the asset refers to different levels of desirability related to levels of potential impacts that might be achieved with successful exploitation. Asset attractiveness is characterized on the scale listed in Table C.10.1.

<b>Table C.10.1 Asset Attractiveness Scale</b>		
<b>Asset Attractiveness</b>	<b>Scale Value</b>	<b>Example</b>
Extremely attractive	5	Potentially devastating economic and public confidence impacts
Very attractive	4	Potentially substantial economic impacts and public confidence impacts
Attractive	3	Potentially significant economic impacts and regional public confidence impacts
Less attractive	2	Potentially nonnegligible economic impacts and some local bad publicity

Table C.10.1 Asset Attractiveness Scale		
Asset Attractiveness	Scale Value	Example
Unattractive	1	Potentially modest economic impacts and some inconvenience for the company

4. **Level of consequence.** This characteristic refers specifically to different levels of potential economic consequences. Level of consequence is characterized on the scale listed in Table C.10.2.

Table C.10.2 Level of Consequence Scale		
Consequence Level	Scale Value	Example (exploitation potential)
Catastrophic	5	More than \$1 billion
Very high	4	\$100 million to \$1 billion
High	3	\$10 million to 100 million
Serious	2	\$1 million to 10 million
Modest	1	Less than \$1 million

5. Likelihood of **preventing an aggressor<sup>1</sup> attempt** before ( $P_b$ ) and after ( $P_a$ ) the recommendation is implemented.<sup>2</sup> (Note that the recommendation may have little or no effect on preventing attempts).
6. Given an attempt, the likelihood of **preventing an aggressor success** before ( $S_b$ ) and after ( $S_a$ ) the recommendation is implemented.<sup>3</sup>

<sup>1</sup>The term *aggressor* here includes not only individuals or groups of individuals who have malicious intent, but also individuals or groups of individuals who may unwittingly or nonmaliciously cause damage to an asset.

<sup>2</sup>The definitions of these probabilities are a bit complex and require a careful reading. The wording asks for probabilities of *preventing* (an attempt or success) before and after implementing a recommendation. So, if a recommendation is effective, it will be more likely to prevent an aggressor's attempt (and/or success, given an attempt) *after* implementing the recommendation. Although the wording is a bit complex, there is a compelling reason for choosing it: the probability of an attempt is something that local law enforcement or corporate security might know about (information that would be addressed in Step 3 of the process shown in Figure 11.1), but the assessment team would not. However, the hope is that it would be possible for the assessment team to think about preventing an attempt, given that someone may be thinking about trying. In many cases,  $P_b$  should be low – maybe even 0. For example, a transformer out in the country is an easy target, and there rarely are any significant “obstacles” that would discourage an aggressor from trying to do harm. In this case, interfering with line-of-sight to the transformer (e.g., by installing a screen, a barrier, or a berm) could have two benefits: it could discourage an attempt and it could make it harder for an aggressor to hit the asset even if he or she went forward with his action; in such a case,  $P_a > P_b$  and  $S_a > S_b$ .

<sup>3</sup>Refer to the footnote for  $P_a$  and  $P_b$ , which are the main variables for characteristic 7.

7. The **technical and cultural difficulty** associated with implementation of the recommendation. This characteristic refers to the possibility that the recommendation may make good sense but requires some cultural adjustments to be effective (e.g., many individuals resisted wearing automobile seatbelts for years until, in some cases, the data on benefits became clear or, in other cases, state law mandated use of seatbelts). Technical and cultural difficulty is characterized on the scale in Table C.10.3.

<b>Scale Level</b>	<b>Description</b>
5	Major system modifications and operating practice revisions
4	Significant training and system modifications required
3	Modest attention and study required for proper implementation and operation
2	Minimal problems
1	No problem

8. **Dependency on other infrastructures.** This characteristic refers to the extent to which the recommendation changes dependencies on other nonenergy infrastructures, including telecommunications, water, road, rail, emergency services, banking and finance, and government services. In addition, this measure addresses the change in dependence between the energy infrastructures (e.g., natural gas or electricity and vice versa).

<b>Scale Level</b>	<b>Description</b>
5	Large increase in dependency
4	Small increase in dependency
3	No change in dependency
2	Reduces dependency
1	Greatly reduces or eliminates dependency

The task leaders are encouraged to list not only those recommendations for consideration that make immediate sense from their perspective, but also recommendations that may further reduce risk but seem too expensive given current circumstances. In such cases, the entire list of recommendations should be examined now and again in future evaluations when conditions may have changed enough (e.g., increased threat) so that some recommendations might then be cost-effective.

As a result of the risk characterization process, some additional observations have been made with respect to:

1. Recommendations that appear to be of particular merit,
2. The existing risk management process at utility, and
3. Potential follow-up activities.

### Presenting Recommendations

Just describing the recommendations with respect to the characteristics is a major step toward structuring the findings of this effort. In addition, some groupings and observations have been made with respect to recommendations that have high-consequence potential or are likely to have low costs to implement. A large number of recommendations are presented, some of which may become more desirable in the future (e.g., after an event that affects another utility).

The recommendations listed in Table C.10.5 address various types of activities. They can be sorted into categories, where one recommendation may address more than one category, as shown in Table C.10.6.

<b>Recommendation Description</b>	<b>Implementation Cost (\$K)<sup>4</sup></b>	<b>Implementation Time (weeks)</b>	<b>Change in Operating Cost (\$K/yr)<sup>a</sup></b>	<b>Attractiveness of Asset</b>	<b>Consequence Level</b>	<b>P<sub>B</sub></b>	<b>P<sub>A</sub></b>	<b>S<sub>B</sub></b>	<b>S<sub>A</sub></b>	<b>Technical &amp; Cultural</b>	<b>Infrastructure Dependency</b>
-----------------------------------	--	------------------------------------	--	--------------------------------	--------------------------	----------------------	----------------------	----------------------	----------------------	---------------------------------	----------------------------------

<b>Category</b>	<b>Number of Recommendations</b>
Policy and/or procedures	
Software	
Hardware	
Studies	
Training	

<sup>4</sup>Effort costs are estimated to be \$10K per person-month.



judge that current conditions do little or nothing to discourage or deter attempts and that implementation of the recommendations would greatly improve the probability of preventing an attempt.

**Table C.10.8 Recommendations with the Largest Increases in Probability of Preventing an Aggressor Attempt**

	Recommendation Description	$P_b$	$P_a$	$P_a - P_b$
--	----------------------------	-------	-------	-------------

Large Increase in Probability of Preventing Aggressor Success, Given an Attempt Is Not Prevented

Some recommendations are thought to be particularly beneficial in preventing aggressor success, given an attempt is not prevented. As in the previous discussion, some task leaders are more optimistic than others that their recommendations would significantly affect this criterion. From the list of recommendations, determine how many, for example, that will have  $S_b - S_a$  values  $\geq 0.6$ .

**Table C.10.9 Recommendations with the Largest Increases in Probability of Preventing Aggressor Success, Given an Attempt Is Not Prevented**

	Recommendation Description	$S_b$	$S_a$	$S_b - S_a$
--	----------------------------	-------	-------	-------------

Asset Attractiveness

Another way to prioritize recommendations is to take those that are judged to be extremely attractive (5 on the scale in Table C.10.11). How many recommendations addressed assets that are considered very attractive (4 on the scale) versus recommendations that are in the 1-5 range? Table C.10.10 only lists recommendations that address extremely attractive assets.

**Table C.10.10 Recommendations That Address Extremely Attractive Assets**

	Recommendation Description	Attractiveness of Asset <sup>a</sup>
--	----------------------------	--------------------------------------

<sup>a</sup>A 5 denotes an extremely attractive asset.

Large Consequences

How many recommendations addressed assets that are judged to be associated with catastrophic (> \$1 billion) consequences (5 on the scale in Table C.10.2) and recommendations addressed assets that are judged to be associated with very high (\$100 million to \$1 billion) consequences (4 on the scale in Table C.10.2)? In addition, how many recommendations are associated with

consequence levels in the 1 to 5 range and are judged to be in the 1 to 4 range? Table C.10.11 only lists recommendations that address catastrophic or very high consequence levels. A range is utilized for some recommendations that addressed impacts that could affect individual users, local systems, or company-wide systems.

**Table C.10.11 Recommendations that Address High-Consequence Assets**

	Recommendation Description	Consequence Level <sup>a</sup>
--	----------------------------	--------------------------------

<sup>a</sup>A 5 denotes a value greater than \$1 billion, and a 4 denotes a value of \$100 million to \$1 billion.

### High Benefit-Cost Ratio

The concept of a benefit-cost ratio is desirable because it provides a “value free” way to combine several of the criteria used to characterize recommendations. Specifically, it includes the cost information (both implementation and operating costs), the before and after probabilities of preventing an attempt and preventing success, and the consequence level.

Calculation of a benefit-cost ratio requires definition and determination of benefits and costs. For this assessment, the benefit is defined as the reduction in expected damages attributable to implementation of a recommendation. The cost of a recommendation is the sum of the implementation cost and the net present value of recurring (annual) costs.

Figure C.10.1 indicates how to calculate expected damages before and after a recommendation is implemented. The top half, which addresses the situation before implementing a recommendation, indicates that there is an unknown probability A that an aggressor intends to attack an asset. If there is no intention, there can be no damage. Given intention, conditions surrounding the asset can either prevent an attack (with probability P<sub>b</sub>), which does not result in damage), or fail to prevent an attack (with probability 1-P<sub>b</sub>). Given that circumstances do not prevent an aggressor’s attempt, circumstances can either prevent success (with probability S<sub>b</sub>), which does not result in damage), or fail to prevent success (with probability 1-S<sub>b</sub>). Therefore, the expected damage level before implementing the recommendation is:

$$D_b = A * (1 - P_b) * (1 - S_b) * (\text{Asset Value}).$$

The bottom half of Figure C.10.1 addresses the situation after implementing a recommendation. The unknown probability A that an aggressor intends to attack an asset is the same as that before implementing a recommendation and the logic is also the same. Therefore, the expected damage level after implementing a recommendation is:

$$D_a = A * (1 - P_a) * (1 - S_a) * (\text{Asset Value}).$$

The benefit, B, of implementing a recommendation is the difference between D<sub>a</sub> and D<sub>b</sub>:

$$B = D_b - D_a.$$

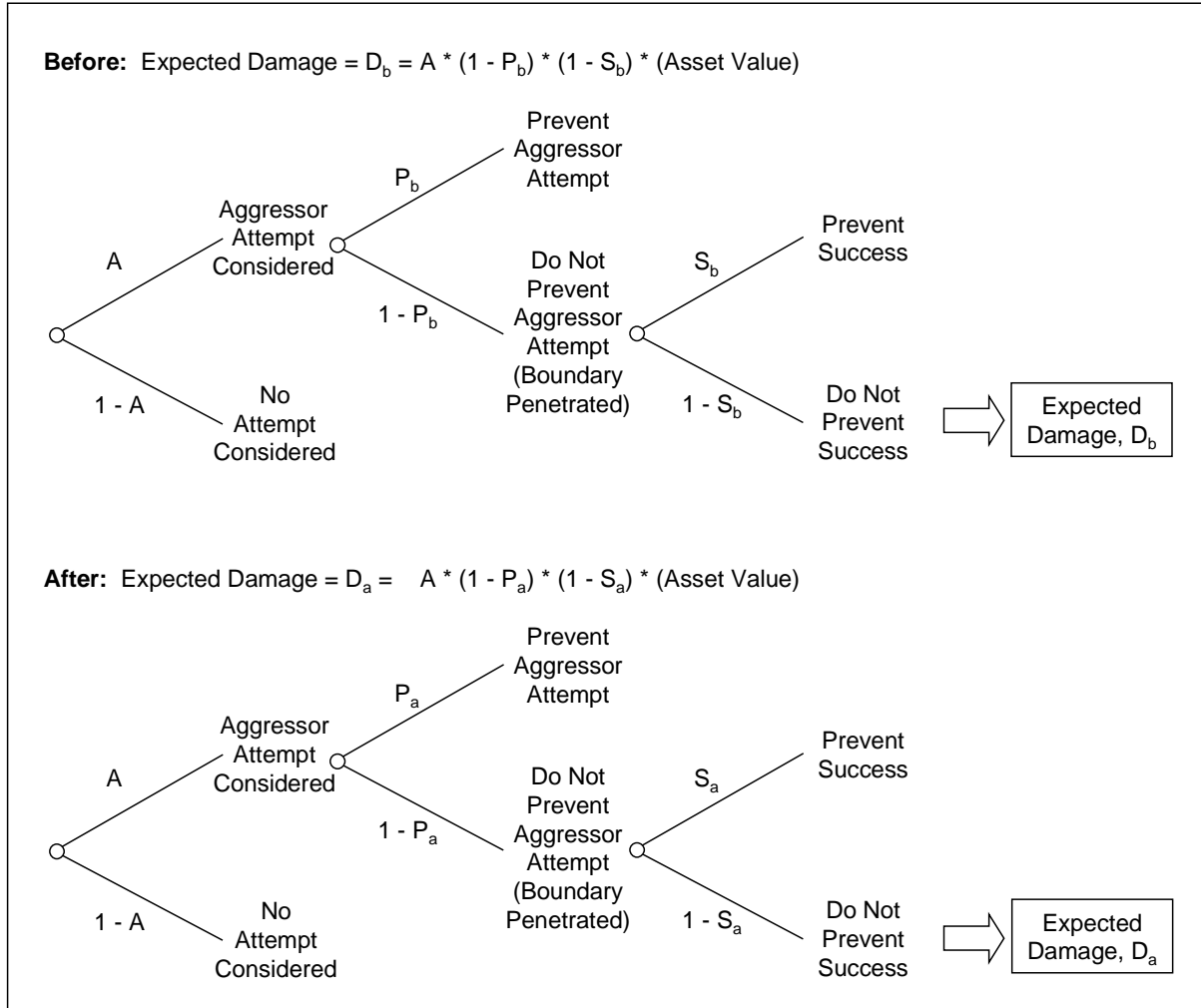
Finally, to get a variable-free (i.e., numeric) value for B, the value of A is momentarily set at 1 and the asset value is set at the consequence level addressed by a recommendation. This results in an upper bound on the benefit-cost ratio.

A recommendation having  $B < 0$  cannot be justified on the basis of this type of an analysis. Other factors could override the effects of  $B < 0$ .

The cost, C, to implement a recommendation is the sum of the implementation cost, IP, and the net present value (NPV) of recurring operating costs (OC):

$$C = IP + NPV(OC)$$

To perform NPV calculations, the cost of capital is set at 7% and the time horizon is set at 10 years. The results of the calculations are shown in Table C.10.X. Two numbers are listed for each recommendation – the benefit-cost ratio and  $A_{crit}$ .  $A_{crit}$  is the value of A, the unknown probability of an aggressor attack that is set to 1, which makes benefits equal to costs. It happens that  $A_{crit}$  is the reciprocal of the benefit-cost ratio. It provides insight into the significance of the benefit-cost ratio because it can be argued that if the actual value of A is judged to be  $> A_{crit}$ , the recommendation is worth implementing.



**Figure C.10.1 Estimating Expected Damage to Assets**

Determine which recommendation has the highest benefit-cost ratio (about 1,300,000) and the smallest  $A_{crit}$  ( $8 \times 10^{-7}$ ). Recall that the costs for this recommendation are on a per user basis. If 1,000 users contribute to the cost, the benefit-cost ratio becomes 1,300 and  $A_{crit}$  becomes  $8 \times 10^{-4}$ . Several recommendations have benefit-cost ratios greater than 1,300.