

VULNERABILITY ASSESSMENT AND SURVEY PROGRAM

Overview of Assessment Methodology



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

September 28, 2001

CONTENTS

1	Introduction.....	1
2	Assessment Methodology.....	3
3	Pre-Assessment.....	6
4	Assessment.....	8
5	Post-Assessment.....	12
6	Summary.....	13

FIGURES

1	Vulnerability Assessment Phases.....	5
---	--------------------------------------	---

1 INTRODUCTION

1.1 OBJECTIVE

This report provides a high-level overview of the vulnerability assessment methodology that is being developed and validated by the U.S. Department of Energy's Office of Energy Assurance (OEA) as part of its multifaceted mission to work with the Energy Sector in developing the capability required for protecting the nation's energy infrastructures. Over the last three 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 and Survey Program 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 documented in related reports.

1.2 BACKGROUND

The U.S. Department of Energy established the Office of Energy Assurance to direct the Department's activities in accordance with Presidential Decision Directive 63 (PDD-63) and the priorities established by the Secretary of Energy. A primary mission of the Office 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.

The vulnerability assessments and surveys are 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, partner's 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 an assessment methodology with associated tools to assist in the implementation; provide training and technical assistance; and stimulate action to mitigate significant problems.

Eleven voluntary assessments have been completed under this initiative (several more are in progress and in the planning stages). The initial assessments focused on the electric power industry, with efforts aimed at the broadest level of the industry. Assessments addressed key energy organizations whose operations, if disrupted, would have broad regional or national

impact. More recently, assessments have included the natural gas industry, and discussions have begun with the oil industry.

1.3 REPORT ORGANIZATION

The remainder of this report is organized as follows. Section 2 discusses the motivation for the program and provides an overview of the three steps in the assessment process—pre-assessment, assessment, and post-assessment. Sections 3-5 discuss each of these steps. Finally, Section 6 summarizes OEA’s strategy for refining and validating the assessment methodology.

2 ASSESSMENT METHODOLOGY

This section discusses the importance of conducting vulnerability assessments and provides an overview of the assessment process and phases.

2.1 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 process of doing an assessment directs senior management attention to security. It surfaces security issues, risks, vulnerabilities, mitigation options, and best practices. Awareness is one of the least expensive and most effective methods for improving the overall security posture of an organization.
- **Establish or evaluate against a baseline.** If a baseline has been previously established, an assessment is an opportunity for a "check up" 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 which serve as a forum for cross-cutting groups to come together and share

issues, experiences, and expertise. External assessors can be instructed to place an emphasis on “teaching and collaborating” versus the traditional role of “evaluator.” Whatever an organization’s current level of sophistication, a long-term goal should be to move the organization towards 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 utilized 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.

2.2 OVERVIEW OF ASSESSMENT PHASES

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 team of national laboratory experts to ensure comprehensiveness and confidentiality of the assessment results. Lessons learned are 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 the 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 1. This includes information gathered through open literature, presentations, classroom instructions, and discussions. In addition, elements of the methodology have been derived from on-going 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 philosophy is to leverage vulnerability assessment techniques, methods, and approaches that have proven to be useful and useable.

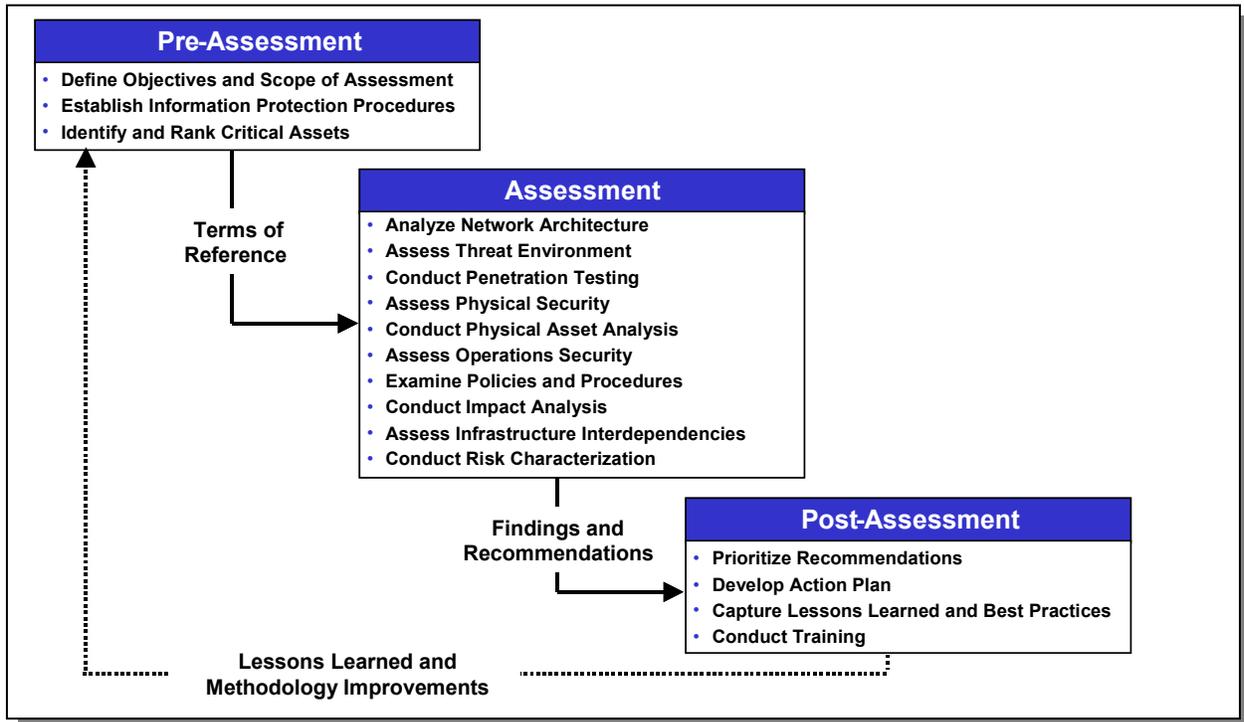


Figure 1 Vulnerability Assessment Phases

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 and cyber—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 1, ten assessment activities are included in the methodology. The appropriateness of each 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 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 an historical perspective and a sense of future plans.
- **Facilitated.** In-house technical experts are used, guided by an outside facilitator. 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, 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.** In this approach, some elements or tasks are performed by internal staff and some are conducted by external experts.

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 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 team conducts an assessment, a non-disclosure agreement (NDA) is typically developed that defines the policies for the storage, transmission, handling, and disposition of all sensitive data gathered and generated during the assessment.

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.

4 ASSESSMENT

As delineated in Figure 1, the assessment methodology consists of ten elements—analyze the network architecture; assess the threat environment; conduct penetration testing; assess physical security; conduct a physical asset analysis; assess operations security; examine policies and procedures; conduct an impact analysis; assess infrastructure interdependencies; and conduct a risk characterization. Each of these elements is described below.

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 to examine includes network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linkage of major software and hardware components (particularly 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, and operating procedures. The assessment should also review existing security plans and analyze results of any prior testing. Results from this element 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.

4.2 THREAT ENVIRONMENT

Developing a clear understanding of threats is a fundamental element of risk management. This understanding, combined with an appreciation of the value of the information assets and systems, and impact of unauthorized access and subsequent malicious activity, provides a basis for better defining the investment that might be prudent to prevent such access. While there are legitimate concerns regarding transnational organizations (e.g., information warfare by intelligence agencies of other nations), the primary focus of this portion of the assessment is those individuals or organizations motivated by financial gain, accomplishing extremist goals (e.g., environmental terrorists or anti-nuclear advocates), embarrassing one or more organizations, or who derive personal pleasure from such penetration (e.g. recreational hackers or disgruntled employees). Characterizing these and other threats, trends in these threats, and ways in which vulnerabilities are exploited should be conducted in this task. To the extent possible, the characterization of the threat environment should be localized to the organization's service area.

4.3 PENETRATION TESTING

The purpose of network penetration testing is to utilize active scanning and penetration tools to identify network vulnerabilities that might be easily exploited by a determined adversary. Penetration testing can be customized to the specific needs and concerns of the utility. In general the penetration testing should include a test plan and details on the rules of engagement for the testing. Penetration testing 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. Lastly, the penetration testing should include identified vulnerabilities and particularly whether access could be gained to the control network or specific subsystems or devices that have a critical role in assuring continuity of service.

4.4 PHYSICAL SECURITY

The purpose of the physical security assessment is to examine and evaluate the physical security systems in place or planned, and to identify potential physical security improvements for the sites evaluated. The 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 (CCTV) (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. The physical security systems are reviewed for design, installation, operation, maintenance, and testing.

The focus of the physical security assessment should be those sites that are directly related to the critical facilities, including information systems and assets required for operation. Typical facilities to include are sites housing 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 based on criteria specified by the organization being assessed.

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. This includes examining asset utilization, system redundancies, and emergency operating procedures. Consideration should be given to the topology and operating practices for electric and gas transmission, processing, storage and delivery, looking specifically for those elements which either singly or in concert with other factors provide a high potential for disruption of service.

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. This is accomplished by identifying, controlling, and protecting generally non-sensitive activities concerning planning and execution of sensitive activities. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and non-sensitive information that might inappropriately aid or abet any individual's or organization's disproportionate influence over system operation (e.g., electric markets or grid operations). This should include review of security training and awareness programs, discussions with key staff, and tours of appropriate principal facilities. It should also include a review of information that may be available through public access.

4.7 POLICIES AND PROCEDURES

The policies and procedures by which security is administered provide the basis for identifying and resolving issues, establishes the standards of reference for policy implementation, and defines and communicates roles, responsibilities, authorities and accountabilities (R^2A^2) for all individuals and organizations which interface with critical systems. They provide the backbone for decisions and day-to-day security operations. The security policies and procedures become particularly important where multiple parties must interact to effect a desired level of security and where substantial legal ramifications may result from policy violations. The policies and procedures should be reviewed to determine whether they (1) address the key factors affecting security, (2) will 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^2A^2 .

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, this will 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 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.

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. This requires a detailed understanding of organization functions, internal infrastructures, and how these link to external infrastructures.

4.10 RISK CHARACTERIZATION

This task 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. This provides a framework to assess 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.

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 first two tasks are aimed at focusing attention on high-priority security concerns and ensuring that these concerns are addressed in systematic and timely manner. As part of OEA's initiative, lessons learned and best practices are captured and disseminated to enhance education and awareness within the energy industry. In the future, training and other technical support activities, such as workshops, will be provided by OEA to supplement the assessment activities.

6 SUMMARY

The draft vulnerability assessment methodology described in this report is being developed by DOE's Office of Energy Assurance to help energy-sector organizations identify and understand the threats to and vulnerabilities of their infrastructures. The methodology is multi-faceted, addressing physical, cyber, and interdependencies-related vulnerability concerns. Through its initiative, the methodology has been successfully applied by a team of experts from DOE's national laboratories to assist Energy Sector organizations in understanding the risks they face, and what steps might be taken to mitigate those risks. The development process is evolutionary in nature, and lessons learned from the assessments, as well as best practice approaches to mitigate vulnerabilities, are documented in related reports.