VULNERABILITY ASSESSMENT AND SURVEY PROGRAM

Lessons Learned and Best Practices

U.S. Department of Energy
Office of Energy Assurance

September 28, 2001

CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE

This report summarizes initial lessons learned and best practices that have been captured as part of a multifaceted effort by the U.S. Department of Energy's Office of Energy Assurance (OEA) 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 performed a series of vulnerability assessments as part of OEA's Vulnerability Assessment and Survey Program. The goal is to help energy-sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures, and to stimulate action to mitigate significant problems. Because the assessments are conducted on a confidential basis, the information in this report is intentionally presented at a high level so as not to reflect on specific companies or industry segments. A separate report entitled *Vulnerability Assessment and Survey Methodology* describes, at a high-level, the methodology developed for the program.

1.2 BACKGROUND

The U.S. Department of Energy established the OEA to direct the Department's activities in accordance with Presidential Decision Directive 63 (PDD-63) and the priorities established by the Secretary of Energy. The 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 assessment and survey program 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, 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 presents and discusses best practices. Section 3 discusses the lessons learned compiled by the vulnerability assessment and survey team. These lessons are organized around the ten interrelated elements of the assessment methodology. Finally, Section 4 provides a summary of this effort.

2 BEST PRACTICES

2.1 BACKGROUND AND SCOPE

Effective operation of the U.S. energy production, transmission, and distribution systems are critical to the health and safety, national security, and economic viability of the nation. Such system operations are becoming increasingly dependent on information systems and other interdependent infrastructures. Even though energy sector information systems have not yet been subject to the same type or intensity of physical and information attacks as other infrastructures, there is growing concern that these systems are becoming more vulnerable. Furthermore, threats associated with critical infrastructures appear to be increasing, thus raising concerns for vital energy infrastructure components and systems. Utility deregulation and advances in technology also contribute to the potential for increased vulnerabilities of our critical energy supply and delivery systems. In addition, as the business model adapts to the new, information-intensive economy, supply chain dependencies increase and interdependencies grow.

The modern energy industry is in the midst of a dynamic era defined by rapid changes in technology (the Internet, information technology), the development of new business models (driven by deregulation, acquisition, and diversification), and the emergence of new internal and external threats (ranging from disgruntled employees to hackers to terrorists). At the same time, there is limited knowledge about threat assessment processes, vulnerability assessment methodologies and tools, and integrated risk management approaches. Descriptions of the new threats and vulnerabilities facing the industry, and recommended actions to address those threats and vulnerabilities, are provided in the recently released North American Electric Reliability Council report *An Approach to Action for the Electricity Sector* and the National Petroleum Council report *Securing Oil and Natural Gas Infrastructures in the New Economy*. The underlying theme in these reports is that vulnerabilities are increasing, they relate to the fundamental evolution of energy enterprises, and holistic efforts are required to address them.

The initial best practices presented below have been assembled as part of the Department's initiative to help energy-sector organizations identify and understand the threats to and vulnerabilities of their infrastructures. They are intended to highlight key issues relating to the protection of the nation's energy infrastructures, and to stimulate action where appropriate.

2.2 BEST PRACTICE RECOMMENDATIONS

To facilitate discussion, the best practices are grouped into three major issue categories: organization, education and awareness, and staffing. In each category, a series of best practice recommendations are stated followed by supporting background information. While the best practices were derived from the vulnerability assessments, they are illustrative, and should not be viewed as comprehensive. That is, because the vulnerability assessments are conducted on a confidential basis, the information is intentionally presented at a high level so as not to reflect on specific companies or industry segments.

Organizational Issues

Organizational issues focus on best practices from a holistic approach. Specifically, they represent activities that should be on going at an enterprise-wide level.

1. **Best Practice: Develop an overarching enterprise security model that is comprehensive, consistent with the mission and values of the organization, and widely accepted within the organization**.
   Organizations should have an overarching security model that integrates both physical and cyber security. A security model establishes the suite of goals that guide development and implementation of security systems, processes, policies, and procedures. The model functionally embodies the risk posture of the organization, at least in the context of security. Such a model enables more balanced decisions on security-based risk acceptance and helps reconcile consideration of competing factors that have an impact on the risk and security condition of the enterprise. Such a model forms the basis for many security-related policies and procedures that can be disseminated throughout the organization. It also is particularly useful when dealing with organizational partners and suppliers.

2. **Best Practice: Develop clear and direct lines of authority with dedicated staff for security, and ensure that responsibility and authority for security is integrated, not dispersed. A strong, accountable advocate at the executive level, with broad corporate acceptance of the role of security in protecting enterprise interests, is vital.**
   Organizations should have dedicated staff with clear lines of authority regarding security that require or at least encourage uniform treatment of security. Many organizations have evolved lines of authority that parse security functions, responsibility, and authority among several organizational elements. This often creates confusion and conflict in developing security policies, their implementation, and administration. Furthermore, it enables (in some cases inspires) some organizational elements to conduct their missions in ways that clearly expose other elements to increased risk. Having dedicated, responsible staff for implementing security is desirable if not essential for effective security.

3. **Best Practice: Incorporate security into enterprise risk management processes.**
   Security should be incorporated into existing risk management processes. For many organizations, risk management is a purely financial function that relates more to acquisitions and mergers, facility siting, safety, or insurance than to asset protection, particularly for information systems. This has two principal impacts. First, security investment decisions lack the benefits that could be provided by a rigorous risk management approach. Second, the lack of integration of security in other risk management investment decisions means that gaps will likely exist in risk acceptance.

Furthermore, investments in vulnerability mitigation will likely be lower than is merited by the risk exposure.

4. **Best Practice: Implement structured security requirements for critical suppliers and partners. Make security reviews an element of contracts for critical services and periodically evaluate compliance.**
   Contracts for supplies and services should include provisions addressing security. The same is true of partnering agreements. Since many of the suppliers, service providers, and partners require either or both physical and electronic access, their vulnerabilities are inherited by the enterprise contacting or partnering with them. Additionally, if the supplies are software, firmware, hardware, or information technology (IT) systems, the capacity to provide secure products or services depends on *their* internal security controls. While traditional remedies exist (e.g., lawsuits and financial losses through degradation of reputation), these are never desired options and they are compromised if there has been no expression of the need for security. Mutual understanding of security expectations at the outset of a relationship is important, and establishing expectations in the original contract will facilitate such understanding and avoid undesirable events and their consequences. The further benefit of establishing such contract requirements is that corporate policies must be established to provide a reasoned basis for establishing expectations of the subcontractor.

5. **Best Practice: Develop a consistent designation and valuation of critical assets, and develop the means to assure the security of these assets.**
   Organizations should establish procedures for identifying critical assets. This is particularly important for information technology assets, which are not as fully understood as physical assets. Understanding asset criticality is important for several reasons. First, decisions regarding protection of enterprise assets are more difficult than for an element of the enterprise because it requires a comprehensive knowledge of all assets to be protected. Second, the likelihood that all employees and partners will have a common appreciation for the importance of an asset is low, making inadvertent loss more probable. Third, the likelihood of human error, particularly by new employees, that compromises an important asset is higher. Lastly, an enterprise often relies upon other infrastructures for support, ranging from law enforcement to telecommunication services.

6. **Best Practice: Carefully consider security issues associated with any organizational changes and communicate the issues to all staff potentially affected by the changes. Make security part of the corporate culture and corporate goals.**
   Organizational change generally increases vulnerabilities. Utilities that change their organizational structures or create uncertainty about such changes are more vulnerable for two reasons. First, clear delineation and universal understanding of roles, responsibilities, authorities, and accountabilities (R^2A^2), as well as organizational functions and processes, are absent following organizational changes. Gaps can develop as the new organization is implemented, creating weaknesses and vulnerabilities that may go undiscovered for lengthy periods. The greater the change in organizational mission or structure, the more profound the potential vulnerabilities and duration of their existence. Second, uncertainty regarding organizational change (especially mission, goals,

functions, etc.) serves to delay implementation of prudent security measures. At a more fundamental level, dysfunctional elements of the organization compound the problem by creating confusion. A culture of security should be developed within the organization.

7. **Best Practice: Monitor security efficiency and performance to ensure a robust security program and to ensure that corporate competitive strategies do not undermine security.**

- Ill-considered competitive strategies can erode security. The energy industry, like other industries, is under pressure to reduce costs. Organizations must be careful as they reduce costs so that they do not also erode security. Outsourcing is one activity that must be carefully considered and structured if security is to be maintained. Mergers and acquisitions increase vulnerabilities during the periods when disparate systems are being integrated, legacy system access is increased, and organizational elements are merged (or discarded). Globalization may decrease costs or offer larger markets, but open enterprises to cultures with different business priorities and motivations. Similarly, internal functions that cannot be directly traced to revenue generation are often targets for cost reduction. Security is rarely viewed as a means to ensure continued revenue flow or growth, but more often as potentially unnecessary or even as an impediment to implementation of low-cost business systems or processes. Finally, downsizing can affect security posture in many ways, such as increasing the pool of disgruntled current or former employees; but principally by reducing the skill level of those entrusted with security functions, or overtaxing the remaining security team.

8. **Best Practice: Periodically review and update emergency plans to include newer threats and vulnerabilities, and test these plans regularly.**
   Emergency plans and business continuity plans need updating and testing regularly through emergency drills and exercises. Employees should be educated about the existence of plans, when they are activated, and what their roles and responsibilities are when they are activated. Because threats and vulnerabilities continue to evolve, these emergency plans should be reviewed, updated, and tested to ensure that these concerns are properly addressed.

9. **Best Practice: Implement appropriate configuration management across all enterprise IT systems. Be particularly attentive to systems that interface with critical assets.**
   Configuration management is crucial even for “non-critical” systems. Absence of good configuration control inevitably opens information networks and systems to vulnerabilities. Lack of adequate staffing, lack of universal awareness of the value of the information and systems, and incomplete, outdated, or unenforced security policies and procedures increase the likelihood that such systems will be violated. The increasing trend to connect administrative computing networks to energy control networks (albeit with safeguards) increases the likelihood that vulnerabilities in non-critical systems will migrate to critical systems.

Education and Awareness Issues

Education and awareness issues focus on activities that organizations can perform to train and educate their employees, contractors, vendors, and customers. These activities, when implemented properly, can cost-effectively increase the level of security across the entire enterprise.

10. **Best Practice: Raise employee awareness to be more proactive on security. Establish and implement policies and procedures for controlling and validating "trust" allocation.**
    Trust is often extended beyond appropriate levels. Industry has enjoyed and valued a culture of trust that is increasingly imprudent, particularly in the cyber dimension. Access to important systems, networks, and facilities should only be granted with due consideration of the need for such access. Increasing threats due to growing competition, erosion of workforce loyalty, growing sophistication of hackers, dependence on contract employees, and outsourcing argue for more discretion and control in assigning trust. Organizations should establish the means to differentiate trust levels and associated accesses and privileges. They should also establish processes to implement that differentiation.

11. **Best Practice: Develop a means to raise and sustain management and employee awareness of physical and cyber threats.**
    Physical and cyber threat awareness needs to be increased enterprise wide. Utilities have only recently begun to experience external cyber attacks, or be the targets of organized groups. For example, the electric power industry has experienced no customer loss of service due to cyber attack. However, major changes in the industry, technology, and society, have created a more hostile world (e.g., the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon). While many organizations understand this and have begun to take steps to address this new world, general awareness and coordinated efforts to ensure protection have not been broadly adopted. In part, the message is that the threats are ubiquitous and growing, but this has not been effectively communicated to the domestic energy industry. Utilities should have programs that increase staff awareness of threats. In general, law enforcement and government have only marginally aided this awareness. They are hindered by a culture that focuses on reaction rather than prevention, and secrecy rather than communication. These cultures are changing, but slowly. Existing communications mechanisms (e.g., through NERC and industry security groups) need to be enhanced and new mechanisms need to be established, where necessary, to provide sensitive threat information to industry.

12. **Best Practice: Develop and adopt means to ensure that both reliability and security missions are understood, as well as their respective roles in ensuring enterprise success.**

- Reliability is often confused with security. Reliability is being able to sustain delivery of service with few and/or minor disruptions. Security however protects the means to provide such reliability as well as achieve the many other desired outcomes of the enterprise (e.g., stockholder confidence, profitability, growth, customer loyalty, positive brand image). Many people in the energy industry confuse these two topics. Indeed, one of the common terms in assuring electric reliability is "security" (basically, the ability of the electric grid to withstand some level of disruption and still function effectively). Since reliability is predominantly defined by natural events, human error, or random equipment failure, few pay significant attention to potential for malicious events and coordinated attacks (particularly when the history of the industry is one of relatively little domestic malicious activity, and essentially no terrorist activity).

13. **Best Practice: Senior management should be periodically briefed and trained on information systems technology and their security, as well as risk management methodologies, analysis, and tools.**
    "New economy" vulnerabilities are elusive for management. The explosion of information technology and its use in vital business functions, has created a knowledge and experience gulf between those in senior management, many of whom have little experience with such technologies, and those younger managers who have such experience. Many senior managers, faced with decisions regarding the myriad of risks they do understand, have difficulty allocating the resources (organizational, managerial, and monetary) to addressing information security challenges that they do not understand. The challenge of information security is educating senior decision makers on the information technologies employed, the vulnerabilities their use presents, and the means to mitigate risks associated with those vulnerabilities.

Staffing Issues

Staffing issues focus on the difficulty of obtaining the right mix of physical and IT security staff.

14. **Best Practice: Security training should be supported as a vital element of risk reduction. Participation in associations advancing security knowledge should be encouraged.**
    The energy industry is suffering from the same shortage of skilled information security staff as all other organizations. Many organizations have resorted to "home grown" information security expertise. While many of these staff are committed, talented, and knowledgeable people, unless large investments in training are made, these individuals can have significant gaps in their knowledge and experience. Even staff assigned traditional security functions (such as physical security) can suffer from inadequate training, particularly in small organizations.

3 LESSONS LEARNED

In addition to the best practices described in Section 2, the assessment teams have documented a number of lessons learned that correspond to each of the ten interrelated elements of the assessment methodology. These elements are: 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. In most cases, these lessons illustrate and highlight the best practices. They are presented to stimulate industry thinking towards more secure infrastructures as new threats and vulnerabilities evolve and as old threats and vulnerabilities resurface.

3.1 NETWORK ARCHITECTURE

- The corporate network of the modern utility has numerous external connections to public and private networks. Connections are used to communicate with customers and offer new electronic services such as online bill presentment and payment. Cyber security should be a primary concern of utilities operating in this new interconnected environment. An enterprise-wide IT security architecture should be developed.

- LAN/WAN networks and system architectures should be documented fully.

- The trend in IT is to outsource more and more functions. Cyber security, however, should remain as an enterprise function, and not become a contractor function.

- Logging and reporting should be enabled on routers and firewalls to gain a better understanding of remote systems and user access.

- Mission critical systems should be identified, and scanning should be performed on these systems. In addition, intrusion detection should be used to detect both internal and external intrusions into critical network systems. Additional layers of security should be included with critical systems (e.g., SCADA systems).

3.2 THREAT ENVIRONMENT

- Disenchanted current and discharged employees pose a significant threat to utilities.

- Criminal threats need to be considered (both organized crime and white-collar crime).

- Background investigations for new hires and periodic updates for current employees can assist in avoiding problems.

- Increased coordination with local law enforcement agencies can assist utilities in better understanding their threats.

3.3 PENETRATION TESTING

- Sensitive and confidential documents should not be placed on websites. Appropriate document review, classification, and access controls should be implemented. This also applies to documents and other information that is found in newsgroups, media sites, and other linked sites.

- Security measures such as traffic filtering, authorized controls, encryption and access controls, minimizing or disabling of unnecessary services and commands, minimizing banner information, and email filtering and virus control should be implemented.

3.4 PHYSICAL SECURITY

- A formal physical security program is essential. Such a program should include listing critical assets, developing a mission statement, defining threats, defining acceptable risks, and applying a vulnerability assessment methodology.

- A formal process for accessing relevant threat information and for contacting the proper law enforcement agencies should be instituted (if it does not already exist) and reviewed and updated on a regular basis. Industry needs to work with government to obtain security clearances for appropriate personnel.

- Appropriate security measures (e.g., access controls, barriers, badges, intrusion detection devices, alarm reporting and display, closed circuit television cameras, communication equipment, lighting, and security officers) should be implemented.

- Top management support is critical in ensuring a successful security program.

- Security training programs should be formalized.

- Procedures for escorting contractors into sensitive areas should be enhanced.

- Security should be incorporated in the company goals as well as in its corporate culture.

3.5 PHYSICAL ASSET ANALYSIS

- Capital expenditures for physical security should be compared to other capital expenditures to ensure proper levels of investment.

- Companies should compare their operating procedures with best practices and procedures used by other industry members to ensure efficiency, reliability, and security.

3.6 OPERATIONS SECURITY

- A five-step program of identifying critical assets, analyzing threats, analyzing indicators and vulnerabilities, assessing risk, and applying appropriate countermeasures should be implemented to enhance the security of a company's sensitive assets.

- The foundation for security is well-informed employees acting responsibly.

- A formal review process should be established for all information released to the public, particularly through the company's web site. A periodic review of "public" information should be performed to audit performance.

- A utility should be particularly careful about the loss of sensitive information to the press or competitors. Information available on personnel (especially executives) should be minimized.

- Security training and awareness should be provided to all employees on a regular basis.

- At a minimum, an annual audit of overall security should be conducted.

3.7 POLICIES AND PROCEDURES

- Formalized policies and procedures provide a foundation for achieving the desired level of security.

- Security policies and procedures need to be promulgated and integrated throughout the organization. Inconsistencies, confusion, and ultimately security gaps can result if business units or sub-organizational groups establish their own policies and procedures.

- Awareness training and education should include security polices and procedures.

3.8 IMPACT ANALYSIS

- Estimates of the potential consequences, including economic implications, of not mitigating identified vulnerabilities or addressing security concerns are necessary in order to effectively apply risk management approaches to evaluate mitigation and security recommendations.

- Outages resulting from a security failure(s) can lead to degradation of company reputation and loss of business in a competitive marketplace.

3.9 INFRASTRUCTURE INTERDEPENDENCIES

- Interdependencies among the infrastructures must be thoroughly investigated because they can create subtle interactions and feedback mechanisms that often lead to unintended behaviors and consequences. Problems in one infrastructure can cascade to other infrastructures.

- Interdependencies increase the complexity of the infrastructures and introduce additional vulnerabilities.

- Interdependencies among the infrastructures vary significantly in scale and complexity, and they also typically involve many system components. The process of identifying and analyzing these linkages requires a detailed understanding of how the components of each infrastructure and their associated functions or activities depend on, or are supported by, each of the other infrastructures.

- Contingency and response plans need to be evaluated from an infrastructure interdependencies perspective and coordination with other infrastructure providers needs to be enhanced.

3.10 RISK CHARACTERIZATION

- A more complete understanding of risk and risk management, as well as more effective risk communication, is needed at all levels of management.

- A risk management process needs to address the costs, benefits, and uncertainties associated with security and vulnerability mitigation recommendations. Such information will aid in establishing priorities and developing a defensible plan of action.

- The risk management process for addressing security concerns should be integrated into the corporate risk management process.

4 SUMMARY

The initial lessons learned, best practices, and observations presented in this report are intended to highlight key issues relating to the protection of the nation's energy infrastructures, and to stimulate action where appropriate. The information was assembled as part of the Department's vulnerability assessment and survey initiative to help energy-sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures. Additional lessons learned and best practices are being captured and documented by the national laboratory team as part of the on-going assessment program, and this draft report will be periodically expanded and enhanced to disseminate relevant information.

On the basis of the eleven assessments that have been conducted, it is clear that comprehensive vulnerability assessments can play a major role in helping energy organizations identify and address risks. It is also clear that such assessments should be conducted on a regular basis to identify new vulnerabilities that may have emerged as a result of the changing threat environment and efforts by organizations to evolve in the competitive marketplace.

The energy industry is not alone in facing these risks. Many of the same vulnerabilities would likely be identified in the other critical infrastructures (e.g., water supply systems, telecommunications, transportation, banking and finance, and emergency and government services). Nevertheless, the industry as a whole would benefit from more concerted attention to common vulnerabilities, particularly those that cross enterprise boundaries. This includes addressing interdependencies with the other critical infrastructures, which adds a whole new dimension to the risk equation. The development and application of risk management methodologies and tools that explicitly incorporate security should be a high priority.