Draft Version 1

Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities

U.S. Department of Energy
Office of Energy Assurance

August 19, 2002

Contents

1 Introduction

The security, economic prosperity, and social well being of the United States depend on a complex system of interdependent infrastructures. Key among these is the energy infrastructure, the electric power, oil, and natural gas production, transmission, storage, and distribution systems—large and small—that fuel and power the economy.

Working through the states and with industry, the Department of Energy's Office of Energy Assurance (DOE/OEA) is responsible for coordinating the federal government's effort to ensure a secure and reliable flow of energy to America's homes, industry, public service facilities, and the transportation system. As part of its multifaceted mission, OEA conducts analyses of physical and cyber vulnerabilities of the national energy infrastructure and develops scientific and technological solutions to correct or minimize system vulnerabilities.

To achieve the goal of protecting our nation's critical energy infrastructure, OEA is developing an integrated federal, state, local, and industry vulnerability mitigation and consequence management architecture. The purpose is to encourage each component of the energy infrastructure to implement a risk management program that starts with a vulnerability analysis and risk assessment, and results in the implementation of appropriate vulnerability mitigation measures. OEA's goal is to include all types and sizes of energy facilities that make up the U.S. energy infrastructure in this integrated risk management architecture. However, small and medium sized energy facilities (e.g., some municipal utilities, independent utilities, and rural cooperatives) without a large corporate parent company often do not have the human resources and financial means to implement a full risk management program.

The purpose of this document is to provide some general guidance and a starting point so that a smaller energy facility is able to identify its critical functions and assets, become aware of threats and vulnerabilities, evaluate and rank the threats in terms of the incidents they may cause, and initiate a security enhancement program, if appropriate. An asset of an energy facility is any person, equipment, material, information, installation, or activity that has a positive value to the facility. A threat is any indication, circumstance, or incident with the potential to damage disrupt an asset. An incident with the potential to cause the loss of or damage to an asset is referred to as an undesirable event. Undesirable events can be due to actions such as theft, compromise, destruction, sabotage, assault, assassination, and kidnapping or due to occurrences such as non-availability or impaired operation of an asset. A vulnerability is any weaknesses that can be exploited by an adversary to initiate an undesirable event that damages or disrupts an asset.

1.1 Why Implement a Risk Management Program?

Risk is a measure of the potential for damage or loss of an asset that will adversely affect the ability of an organization to function properly or a mission to be carried out. The level of risk or risk rating of an asset is a function of two factors: (1) the value placed on the asset by its owner because of the consequences of a loss or disruption of that asset and (2) the likelihood that a specific vulnerability the asset will be exploited by a particular threat. The likelihood that a specific vulnerability will be exploited by a particular threat depends on the nature of the vulnerability and the level of the threat.

A risk management program provides a framework within which assets and their criticalities to an organization or mission are quantified, threats to these assets are characterized, and the vulnerabilities of the assets to the threats are analyzed. A full risk management program also provides a framework within which the resulting risks are assessed and ranked, possible mitigation options to reduce vulnerabilities (and thus risks) are identified, and appropriate options are selected and implemented to achieve and acceptable level of risk at an acceptable cost. Vulnerability analyses and risk assessments can assist in identifying the criticality of assets (or the impact of their loss) and existing threats and vulnerabilities. The tools of risk management also address the costs, benefits, and uncertainties associated with implementing recommendations involving security and vulnerability mitigation. Such information will aid in establishing priorities and developing a defensible plan of action.

1.2 Checklist Concept

Various approaches to the risk management process have been developed for various situations. DOE has developed an initial step-by-step checklist approach to the risk management process for energy infrastructures and major energy companies. In this document, this checklist approach is adapted for use by small and medium sized energy facilities, such as some municipal utilities, independent utilities, and rural cooperatives. It includes an overview of a fairly standard, top-level approach to the concepts of vulnerability analyses and risk assessments and lists of questions and considerations for use during each major step of the overall risk management process. The purpose is to assist operators of small and medium sized energy facilities in identifying priorities for protecting their local individual portions of the nation's energy infrastructure.

The appendix contains a list of definitions of key terms used in the risk management discipline and a list of nomenclature used in this document.

2 Risk Management Overview

2.1 Coordination of a Risk Management Program

Before the establishment of an energy infrastructure risk management program, the resources required to implement such a program should be identified, the present status of any existing infrastructure protection programs or procedures should be determined, and procedures to identify the critical assets of the infrastructures and to quantify risks associated with them should be established.

Along with a basic understanding and knowledge of the term risk and the risk management process, coordination is an important ingredient in a successful risk management program. An energy facility should work closely with industry associations (e.g., National Rural Electric Cooperative Association, American Public Gas Association) and with federal, state, and local governments and law enforcement agencies.

The energy facility should consider identifying the following to assist in coordination efforts:

- existing help that is available from industry associations, larger energy companies, and federal, state, and local governments, regulating agencies, and law enforcement agencies for conducting an integrated vulnerability analysis and risk assessment of the energy facility;
- protection and security assurance responsibilities at the federal, state, and local levels;
- protection and response resources at the federal, state, and local levels that could be integrated with the resources of the first responders at the energy facility;
- technical and resource needs available from federal, state, and local agencies and industry associations for supporting vulnerability analyses, risk assessments, risk management, consequence mitigation activities, and education and training;
- common security requirements for energy systems (e.g., those adopted uniformly and consistently throughout the United States) that might be available from industry associations;
- information-distribution processes for sharing threat notifications, warnings, and alerts with neighboring energy facilities, energy associations, and local, state, and federal governments;
- formal mutual assistance agreements at the federal, state, and local levels with government agencies and larger energy companies to support response, repair, and restoration activities if an energy facility is disrupted; and
- processes to identify interdependencies among the infrastructures and assess the need for emergency or redundant backup systems.

Several of these items are complex and would require cooperation among the energy industry and all levels of government. Although energy facilities are responsible for their own risk management, local and state governments need to take a proactive role to help these facilities perform the needed risk assessments, adopt adequate and cost beneficial methodologies, and take actions to address the findings.

Through its Vulnerability Survey and Analysis Program, DOE has developed a risk management methodology along with lessons learned and best practices. Small and medium sized energy facilities, along with local governments and appropriate industry associations, can use an adaptation of this methodology as a starting point to help assess their current situation and develop action plans.

The next section presents an outline of a typical risk management process, which is described further in Section 3. Before applying a risk management process to an energy facility or other organization, it is prudent to conduct a preliminary review of the facility or organization's mission and mission support documents and information. Relevant information about critical information, systems, and assets could include:

- relative priorities or importance over time;
- interrelationships and interdependencies with other infrastructures and organizations;
- logical, physical, and functional network and system diagrams;
- blueprints, user's manuals, and architectures of systems or assets;
- purposes; and
- concepts of operation (e.g., operations manuals or procedures).

Other information about the facility or organization that is germane to a risk assessment includes:

- previous vulnerability analysis or risk assessment results and reports;
- relevant policies and procedures (e.g., security or emergency preparedness procedures);
- continuity of operations, contingency, disaster recovery, and backup plans or procedures; and
- dependence on other organizations or systems (e.g., supervisory control and data acquisition [SCADA] systems, telephone and fiber-optic line connectivity, utilities, government services).

The facility or organization should also consider preliminary information on the following:

- its perception of the primary threats to critical mission and mission support information, systems, and assets;
- the types of threats, such as insider (by malicious act, espionage, or theft of property or sensitive information using their special access, knowledge, or privileges), terrorist (by bombing, kidnapping, or biological, chemical, or nuclear attacks), foreign or industrial intelligence (including hackers), environmental (from fires, storms, flood, tornados, or pollution), criminal (by theft, destruction or property, or violent acts against people with or without collusion with an insider), or military (using conventional, biological, chemical, or nuclear warfare); and
- the anticipated threat tactics, such as social engineering or collusion, stealth, brute force, physical attack and damage, open-source research, or third-party usage.

2.2 Outline of Risk Management Steps

This section presents an outline of the risk management process proposed for small and medium independent energy facilities which has been adapted from the initial DOE-developed step-by-step checklist approach to the full risk management process.

Step 1. Identify critical assets and the impacts of their loss.

1.1 Identify the critical functions of the energy facility.
1.2 Determine which assets perform or support the critical functions.
1.3 Evaluate the consequences or impacts to the critical functions of the facility from the disruption or loss of each of these critical assets.

Step 2. Identify what protects and supports the critical assets.

2.1 Identify the components of the physical security system (e.g., perimeter barriers, building barriers, intrusion detection, access controls, and security forces) that protect each asset.
2.2 Identify the critical internal and external infrastructures (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset.
2.3 Identify sensitive information about the energy facility and its operation that must be protected.

Step 3. Identify and characterize the threat.

3.1 Gather threat information and identify threat categories and potential adversaries.
3.2 Identify the types of threat-related undesirable events or incidents that might be initiated by each threat or adversary.
3.3 Estimate the frequency or likelihood of each threat-related undesirable event or incident based on historical information.
3.4 Estimate the degree of threat to each critical asset for each threat-related undesirable event or incident.

Step 4. Identify and analyze vulnerabilities.

4.1 Identify the potential vulnerabilities of each asset to each threat or adversary.
4.2 Identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary. (Step 2 provides a stating point for this activity.)
4.3 Estimate the degree of vulnerability of each critical asset for each threat-related undesirable event or incident and thus each threat or adversary.

Step 5. Assess risk and determine priorities for asset protection.

5.1 Estimate the effect on each critical asset from each threat or adversary taking into account existing protective measures and their levels of effectiveness.
5.2 Determine the relative degree of risk to the energy facility in terms of the expected effect on each critical asset (a function of the consequences or impacts to the critical functions of the facility from the disruption or loss of the critical asset, as evaluated in Step 1) and the likelihood of a successful attack (a function of the threat or adversary, as evaluated in Step 3, and the degree of vulnerability of the asset, as evaluated in Step 4).
5.3 Prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks using an integrated assessment.

Step 6. Identify mitigation options, costs, and trade-offs.

6.1 Identify potential mitigation options to further reduce the vulnerabilities and thus the risks.
6.2 Identify the capabilities and effectiveness of these mitigation options.
6.3 Identify the costs of the mitigation options.
6.4 Conduct a cost-benefit and trade-off analyses for the various options.
6.5 Prioritize the alternatives for implementing the various options and prepare recommendations for decision makers.

3 Checklists for Initiating a Risk Management Process at an Energy Facility

The following sections describe the steps of the risk management process outlined in Section 2.2. Where appropriate, the steps contain checklists of questions that could be used to guide the implementation of a risk management program for the energy facility.

3.1 Step 1. Identify Critical Assets and the Impacts of Their Loss

Estimates of the potential consequences, including economic implications, of not mitigating identified vulnerabilities or addressing security concerns are necessary to effectively apply risk management approaches to evaluate mitigation option and security recommendations. Outages because of security failures could degrade an energy facility's reputation and place the community served at risk to economic losses or even losses of property and life.

In addition, the modern energy facility's telecommunication and computer network has many external connections to public and private networks. Such connections are used to communicate with customers and offer new electronic services, such as on-line billing and payment. Cyber security should be a primary concern, especially for utilities that operate in this interconnected environment. An information technology (IT) security architecture may need to be developed.

Possible critical assets include people, equipment, material, information, installations, and activities that have a positive value to an organization or facility. People include energy facility executives and managers, security personnel, contractors and vendors, and field personnel. Equipment includes vehicles and other transportation equipment, maintenance equipment, operational equipment, security equipment, and IT equipment (computers and servers). Material includes tools, spare parts, and specialized supplies. Information includes employee records, security plans, asset lists, intellectual property, patents, engineering drawings and specifications, system capabilities and vulnerabilities, financial data, and operating, emergency, and contingency procedures. In addition to the operational installations that make up the energy infrastructure itself, installations include headquarters offices, field offices, training centers, contractor installations, and testing, research, and development laboratories. Activities include movement of personnel and property, training programs, communications and networking, negotiations, and technology research and development.

The energy facility, the local government, and energy industry associations have roles and responsibilities for identifying assets, effects of asset loss, vulnerabilities, threats, and risk mitigation options. Coordination among energy facilities; local, state, and federal agencies; and energy industry associations is crucial to this process.

Energy facilities need to identify the critical functions of the facility, and determine which physical and cyber assets perform or support the critical functions. The key assets identified should be related to the criticality of overall operations of the individual facilities. Potential assets include substations, transmission lines, pipelines, critical valve nests, power plants, pump stations, city gate stations, compressor stations, storage installations, interconnections, energy control centers, energy management systems (EMS), SCADA systems, remote monitoring and control units (remote terminal units [RTU]), communications systems linking RTUs and energy

control centers, certain backup systems, and e-commerce capabilities. They should evaluate the consequences or impacts to the critical functions of the energy facility from the disruption or loss of each of these critical assets and prioritize the critical assets based on these.

Not all assets and activities warrant the same level of protection. The cost of reducing risk to an asset must be reasonable in relation to its overall value. The value, however, does not need to be expressed in dollars. A potential loss can be stated in terms of human lives or the impact on the local or state economy.

The first set of questions is designed to guide the process of identifying the critical functions of the energy facility and the assets that perform or support them, and evaluating the potential consequences of disruptions or loss of these critical assets.

Criticality Criteria (Functions and Assets)
☐ What critical mission activities take place at the energy facility or its remote sites?
☐ What critical or valuable equipment is present at the facility or its remote sites?
☐ Where are the critical assets located?
☐ Have people, installations, and operations been considered when assessing assets?
☐ Have cyber networks and system architectures (e.g., SCADA systems, business e-mail, and e-commerce) been documented fully?

Criticality Criteria (Impacts of Loss)
☐ What would the energy facility lose if an adversary obtained control of a specific asset?
☐ What affects would be expected if a specific asset were compromised?
☐ Is the asset still valuable to the energy facility once an adversary has it?
☐ What is the potential for immediate and significant local impacts due to the loss of the asset?
☐ What is the potential for loss of energy supply to civilian areas?
☐ What facility personnel, tenants, customers, and visitors could be affected by the loss of the asset?
☐ What would be the impact on people's lives and on national or local security due to the loss of the asset?
☐ What would be the financial impacts to the energy facility and the local community?

Criticality Criteria (Asset Value)
☐ Is there little or no redundant capacity or capability to mitigate the loss of the asset?
☐ What is the potential for cascading effects (e.g., to other interdependent infrastructures or industries) due to the loss of the asset?
☐ Do any special situations need to be considered regarding the loss of the asset, such as the status of hospitals, life support systems, or emergency services that depend on the energy infrastructure supported by the asset?
☐ What is the potential for catastrophic effects (weapons of mass destruction levels impact)?
☐ What did it cost to develop the asset?
☐ Would the energy facility need an extended period to make repairs to the asset?
☐ How does the need for protecting the asset compare with other assets also considered critical?

Once the assets critical to the operation of the energy facility have been identified and characterized, an impact assessment must be carried out to describe the consequences of losses if an undesirable event occurs. The degree of impact should be quantified by using a relative impact or criticality rating criteria and a consistent rating scale. (An example of a scale for rating criteria is presented in Step 5.) The assets are then ranked in terms of criticality.

3.2 Step 2. Identify What Protects and Supports the Critical Assets

The exiting protection of critical assets provided by the physical security system and the dependence of the critical assets on both external and internal infrastructures must be known to evaluate the vulnerabilities of the assets to threats or adversaries. In addition, operating procedures and other sensitive information, which if available to adversaries might jeopardize critical assets, must be identified as their availability can also affect the vulnerabilities of assets.

Physical Security Systems

Physical security systems are used to protect energy facilities and their assets from unauthorized individuals and outside attacks. Such systems usually include perimeter barriers, building barriers, intrusion detection, access controls, and security forces.

Infrastructure Interdependencies

Today's energy facilities depend on many different infrastructures to support their critical functions and assets. These infrastructure interdependencies must be identified and the adequacy of security measures that are in place to protect and back up these infrastructures must be evaluated. Typically, these supporting infrastructures include:

- electric power supply and distribution;
- petroleum fuels supply and storage;
- natural gas supply;
- telecommunications;
- transportation (road, rail, air, and water);
- water and wastewater;
- emergency services (fire, police, and emergency medical);
- computers and servers;
- heating, ventilation, and air conditioning (HVAC) systems;
- fire suppression and fire fighting systems; and
- SCADA systems.

The electric power supply and distribution infrastructure can include the local electrical distribution utility, facility-operated electric generation equipment, backup generators fueled by natural gas or petroleum fuels, uninterruptible power supplies (UPSs), and the associated switching and distribution hardware. The petroleum fuels supply and storage infrastructure includes on-site storage as well as local suppliers, storage terminals, and the entire petroleum industry. The telecommunications infrastructure includes commercial telephone, fiber optic, and satellite networks and facility-owned radio, telephone, microwave, and fiber-optic pathways. Computers and servers, HVAC systems, fire suppression and fire fighting systems, and SCADA systems tend to be operated by the energy facility and, in turn, depend on the other infrastructures such as telecommunication, electric power supply and distribution, petroleum fuels supply and storage, natural gas supply, water and wastewater, and emergency services.

Sensitive Information

Protecting operating procedures and other sensitive information, the release of which might jeopardize an energy facility and its assets, is the objective of operations security (OPSEC) programs. OPSEC programs utilize tools such as employee background checks, trash handling procedures, telephone policies, and IT (computer) security to protect against both industrial espionage and deliberate disruption of critical assets and functions.

The second set of questions is designed to guide the process of identifying the existing components of the physical security system that protect the critical assets, the critical infrastructure systems that support the critical assets, and the operating procedures and sensitive information that must be protected to avoid jeopardizing the critical assets.

Energy Facility and Critical Asset Protection (Physical Assets)
☐ What department or person has overall responsibility for security or is that responsibility spread over many departments or people with shared responsibilities for security along with their other responsibilities?
☐ What perimeter barriers (e.g., fences, gates, vehicle barriers) protect the energy facility as a whole and the individual critical assets and what levels of protection do they provide?
☐ What building barriers (e.g., walls, roof/ceiling, windows, doors, locks) protect each critical asset and what levels of protection do they provide?
☐ What is the status of the intrusion detection that protects each critical asset (e.g., intrusion sensors, alarm deployment, alarm assessment, alarm maintenance) and what level of protection does it provide?
☐ What is the status of the access control that is used at each critical asset (e.g., personnel access, vehicle access, contraband detection, access point illumination) and what level of protection does it provide?
☐ What is the nature of the security force (both the protective force and appropriate local law enforcement agencies) that protects each critical asset (e.g., number, training, armament, communications) and what level of protection does it provide?
☐ What types of undesirable events (e.g., surreptitious forced entry, technical implant, theft of sensitive information or materials) are protected against?
☐ During which hours of the day and under what conditions are the various components of the physical security system effective?
☐ Over what areas do the various components of the physical security system provide protection?
☐ What is the history of reported malfunctions of the various components of the physical security system?
☐ What is the correlation of the effectiveness of the various components of the physical security system to security incident reports that may indicate that the system was defeated?
☐ Have liaisons and working relationships been established with the local government and its departments, such as police, fire, emergency medical services, and public works?

Energy Facility and Critical Asset Protection (Infrastructure Interdependencies)
☐ Which infrastructures (both external and external) are essential for a specific critical asset to be able to carry out its critical functions?
☐ What external utility or internal department and equipment is the normal provider of each essential infrastructure for each critical asset and how is each infrastructure connected to each asset (e.g., the types and pathways of power lines, pipelines, and cables)?

Energy Facility and Critical Asset Protection (Infrastructure Interdependencies)	
☐	What alternatives (e.g., redundant systems, alternative suppliers, backup systems established work-around plans) are available if the normal providers of the essential infrastructures are disrupted and how long can the alternatives support the critical functions of the assets?
☐	What is the potential for interdependency effects on external infrastructures (i.e., effects on the energy, telecommunications, transportation, water and wastewater, banking and finance, emergency services, and government services infrastructures)?

Energy Facility and Critical Asset Protection (Sensitive Information)	
☐	What types of information about the energy facility, its assets, and its operations should be considered critical or sensitive information?
☐	What are the methods and means by which sensitive information might fall in the wrong hands, such as via disgruntled employees; access to the facility by the public; outside construction, repair, and maintenance contractors; press contacts; briefings and presentations; public testimony; Internet information; paper and material waste; telecommunications system taps; and cyber (computer) intrusions?
☐	What are the existing policies and procedures that are used to protect sensitive information, such as employee background checks, disciplinary procedures, security training, trash handling procedures, paper waste handling procedures, salvage material handling procedures, dumpster control, telephone policies, and IT (computer) security.

Once energy facilities have identified their existing physical protective measures, they should coordinate with their respective local governments and law enforcement agencies to ensure that the level of protection and response that they expect will be forthcoming. They should also coordinate with the critical external infrastructure providers to ensure that the robustness and redundancy that they depend on will continue to be provided. The objective of these coordination efforts is to ensure that roles for response and recovery from a disruption are understood by all so that quick and effective measures can be taken when problems occur.

In addition, local and state governments can assist energy facilities in infrastructure restoration activities. Potential support can come in many areas, such as maintaining critical spare parts, assisting with special equipment, working with the emergency telecommunications spectrum, securing easy access to the site of the disruption for repair crews and needed equipment, working out mutual assistance programs with other energy providers, and supplying temporary staffing.

The energy facility should also check with local and state governments to ensure that critical information about their facility, its assets, and its operations will not be released to the general public in any future additions to public Internet sites, press releases, or public hearings.

3.3 Step 3. Identify and Characterize the Threat

In order to put the information about the critical assets of the energy facility gathered above to use in a quantitative risk assessment, the potential threats and adversaries that may be expected must be identified and quantified. The set of questions provided in this section serves as guidance for evaluating the threat environment to which the energy facility could be exposed and establishing qualitative or quantitative threat ratings for each critical asset. The goals of the threat assessment are to understand, from the adversary's point of view, the adversary's capabilities and intent to collect critical information.

The federal agencies (e.g., DOE and the Federal Bureau of Investigation [FBI]), state governments, and energy industry associations each collect threat information. This information should be shared among these groups and with the local energy facilities in order to have the most comprehensive and updated threat information possible. In addition, threats to energy facilities could affect state and local assets. State and local governments have access to law enforcement and intelligence data. This information should be integrated and shared, together with any information that the energy industry associations and energy facilities collect.

This third set of questions is to be used to identify and evaluate the threat environment to which an energy facility may be exposed.

Intent and Capabilities of Adversaries	
☐	What types of adversaries are expected?
☐	Who are the specific adversaries expected?
☐	What are the specific goals and objectives of each adversary?
☐	Which are the critical assets that each specific adversary is aware?
☐	Does each specific adversary know enough about the asset to plan an attack?
☐	What are the possible modes of attack (e.g., explosives or incendiary devices delivered by car, truck, boat, rail, mail, individuals, or standoff weapons; aircraft impacts; sabotage of equipment or operations; assaults by lightly or heavily armed individual attacker or team of attackers; theft, alteration, or release of information, materials, or equipment; contamination by chemical agents, biological agents, or radioactive material; and cyber attacks) each adversary might use?
☐	Are there other, less risky means for a specific adversary to attain his/her goals?
☐	What is the probability that an adversary will choose one method of attack over another?
☐	What specific events might provoke a specific adversary to act?

Information concerning potential threats and adversaries can be gathered about potential threats and adversaries by:

- joining a threat analysis working group that includes local, county, state, and federal agencies, the military, and other industry partners;
- obtaining access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc., (ANSER), FBI-sponsored InfraGuard, Carnegie Mellon University's CERT®, or other information system security warning notices;
- initiating processes to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses, other working groups in the area);
- arranging for threat briefings by local, state, and federal agencies;
- performing trend analyses of historical security events (both planned and actual); or
- creating possible threat scenarios based on input from the threat analysis working group and conducting related security exercises.

3.4 Step 4. Identify and Analyze Vulnerabilities

In addition to identifying the critical assets of the energy facility, the impact of their disruption, the present protection provided, and the potential threats against them, the vulnerability of those assets to the potential threats must be quantified, at least to some extent, to determine the overall risk to the assets.

There are various types of vulnerabilities such as physical, technical/cyber, and operational. An energy facility, including perimeter barriers (fences, walls, gates, landscape, sewers, tunnels, parking areas, alarms), compound area surveillance (closed-circuit television, motion detectors, lighting), building perimeters (walls, roofs, windows, doors, shipping docks, locks, shielded enclosures, access control, alarms), and building interiors (doors, locks, safes, vents, intrusion sensors, motion sensors), is subject to physical vulnerabilities. Electronic equipment, such as acoustic equipment, secure telephones, computers and computer networks, and radio-frequency equipment, are subject to technical or cyber vulnerabilities. The guard force, personnel procedures, and operational procedures are subject to operational vulnerabilities.

Various characteristics of assets, including any existing protection identified in Step 2, may affect their susceptibility to attacks and must be considered when identifying susceptibilities. Such asset characteristics include building design; equipment properties; personal behavior; locations of people, equipment, and buildings; and operational and personnel practices.

Both energy facilities and local governments should be concerned with identifying and analyzing vulnerabilities. Energy facilities should analyze the vulnerabilities of their physical and cyber systems. Local governments should coordinate management of the vulnerabilities of the energy infrastructure, including individual energy facilities, that support government and community operations and assets.

This fourth set of questions is to be used to evaluate the vulnerability of the critical energy infrastructure assets to the potential threats and to establish qualitative or quantitative vulnerability ratings for each asset.

Energy Facility and Critical Asset Vulnerabilities	
☐	How susceptible is each critical asset to physical attack if readily available weapons (guns, normal ammunition, vehicle, simple explosives) were used?
☐	How susceptible is each critical asset to physical attack if difficult-to-acquire weapons (assault rifles, explosive ammunition, rocket launchers, biological or chemical agents, aircraft, sophisticated explosives) were used?
☐	How susceptible is each critical asset to physical attack from insiders?
☐	Are any of the critical assets unprotected? If so, describe them.
☐	Are any of the critical assets minimally protected? If so, describe them.
☐	How susceptible is each critical asset to cyber attack?

3.5 Step 5. Assess Risk and Determine Priorities for Asset Protection

Scales for the rating criteria identified in the first four steps (asset criticality in term of the impact of loss or disruption, threat characteristics, and asset vulnerability) must be developed. The concept of criteria development is presented below in the form of a generic example. Those that conduct an actual assessment should define rating scales that are appropriate to the specific assessment.

Using the individual rating values assigned to each combination of asset criticality, threat, and vulnerability, a relative degree of risk or a risk rating can be established for each asset for one or more postulated adverse events or consequences that could result from an attack by the identified adversary. Often a multiplicative approach involving the three rating criteria is used to obtain a risk rating:

$$\text{Risk Rating} = (\text{Impact Rating}) \times (\text{Threat Rating}) \times (\text{Vulnerability Rating}).$$

An additional scale must be developed to assign a qualitative overall risk level from the quantitative risk rating. The risk ratings or risk levels are used to prioritize the assets for the selection and implementation of security improvements to achieve an acceptable overall level of risk at an acceptable cost.

The following should be considered when developing and using rating criteria.

- Subject-matter expert opinions and perspectives should be documented. The team involved in the assessment should reflect a variety of different perspectives, and the team should work toward reaching a consensus regarding a set of priorities.
- Information should be presented in a usable format (e.g., table, matrix, or spreadsheet).
- Assumptions should be documented.

A generic example of possible scales for the rating criteria is presented below in the form of a set of tables to illustrate the concept. These or similar tables are used to establish qualitative or quantitative criticality, threat, and vulnerability ratings for each critical asset.

Asset Impact/Criticality Rating Criteria

Each critical asset that is identified in Step 1 of the risk management process is assigned an impact rating value that reflects the importance or criticality of a loss or disruption of that asset with regard to the continued operation of the energy facility or other organization being assessed. In the example below, a quantitative criticality rating scale of 0 to 100% is used, which corresponds to qualitative criticality levels of critical, high, medium, and low.

Asset Impact/Criticality Rating Criteria		
Criticality Level	**Description**	**Rating Scale (%)**
Critical	Indicates that compromise of the asset would have grave consequences leading to loss of life or serious injury to people and disruption of the operation of the energy facility. It is also possible to assign a monetary value or some other measure of criticality.	75–100
High	Indicates that compromise of the asset would have serious consequences that could impair continued operation of the energy facility.	50–75
Medium	Indicates that compromise of the asset would have moderate consequences that would impair operation of the energy facility for a limited period.	25–50
Low	Indicates little or no impact on human life or the continuation of the operation of the energy facility.	1–25

Threat Rating Criteria

The individual potential threats against the assets of the energy facility or other organization being assessed that are identified in Step 3 are assigned a threat rating value that reflects the magnitude of the threat. In the example below, a quantitative threat rating scale of 0 to 100% is used, which corresponds to qualitative threat levels of critical, high, medium, and low.

Threat Rating Criteria		
Threat Level	**Description**	**Rating Scale (%)**
Critical	Indicates that a definite threat exists against the asset and that the adversary has both the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis.	75–100
High	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset and based on related incidents having taken place at similar assets or in similar situations.	50–75
Medium	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise the asset and the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents.	25–50
Low	Indicates little or no credible evidence of capability or intent and no history of actual or planned threats against the asset	1–25

Vulnerability Rating Criteria

The vulnerabilities of the assets in terms of in-place measures to protect those assets that are identified in Step 2 are assigned a vulnerability rating value that reflects the extent to which the asset is protected against each threat identified in Step 3. In the example below, a quantitative vulnerability rating scale of 0 to 100% is used, which corresponds to qualitative vulnerability levels of critical, high, medium, and low.

Vulnerability Rating Criteria		
Vulnerability Level	**Description**	**Rating Scale (%)**
Critical	Indicates that there are no effective protective measures currently in place and adversaries would be capable of exploiting the critical asset.	75–100
High	Indicates that although there are some protective measures in place, there are still multiple weaknesses through which adversaries would be capable of exploiting the asset.	50–75
Medium	Indicates that there are effective protective measures in place; however, one weakness does exist that an adversaries would be capable of exploiting.	25–50
Low	Indicates that multiple layers of effective protective measures exist and essentially no adversary would be capable of exploiting the asset.	1–25

3.6 Step 6. Identify Mitigation Options, Costs, and Trade-offs

The ultimate goal of a risk management process is to select and implement security improvements to achieve an acceptable overall risk at an acceptable cost. Step 5 of the risk management process prioritizes the combinations of assets and threats by the risk ratings or risk levels. This, in turn, helps to identify where protective measures against risk are most needed.

In this step, potential measures to protect critical assets from recognized threats are identified, specific programs to assure that appropriate protective measures are put into place are established, and appropriate agencies and mechanisms needed to put protective measures in place are identified. Protective measures that can address more than one threat or undesirable event should be given special attention.

A variety of approaches to developing protective measures exist. Protective measures can reduce the likelihood of a failure due to an attack by adding physical security. Protective measures can also be implemented to prevent or limit the consequences of a failure or to speed the recovery following a failure, no matter what the cause of that failure.

Best practices and lessons learned from DOE's Vulnerability Survey and Analysis Program provide some general actions, activities, and recommendations that can help identify appropriate potential mitigations measures. Some of these are listed below.

- The trend in IT until very recently has been to outsource more and more functions. Since the events of September 11, 2001, outsourcing is becoming less popular again. If possible, cyber security should remain as an enterprise function and should not become a contractor function.

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

- Sensitive and confidential documents should not be placed on Web sites. Appropriate document review, classification, and access controls should be implemented. This practice should apply 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 e-mail filtering and virus control, should be implemented.

- A formal process for accessing relevant threat information and for contacting the proper government and law enforcement agencies should be instituted (if it does not already exist), and reviewed and updated on a regular basis. The energy facility may need 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 and visitors into sensitive areas should be enhanced and enforced.
- Security should be incorporated in the company goals as well as in its corporate culture.
- 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 energy facility's Web site. A periodic review of "public" information should be performed to audit the effectiveness of information protection policies.
- The energy facility should be careful about disseminating sensitive information to the press or competitors. Only minimal information should be made available about personnel (especially executives).
- 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.

Some illustrations specific to energy facilities, including large utilities not specifically considered in this report, are listed below as an example of specific protective measures that can be implemented. The examples are grouped by type.

Measures to Prevent Damage

- Harden key installations and equipment: protect critical equipment with walls or below-grade installations, physically separate key pieces of equipment, and toughen the equipment itself to resist damage.
- Install surveillance systems (e.g., video cameras, motion detectors) around key installations that is monitored and coupled with rapid-response forces.

- Maintain security guards at key installations.

- Improve communication with law enforcement agencies, especially local law enforcement agencies and the local FBI office) to obtain threat information and coordinate responses to emergencies.

Measures to Limit Consequences

- Improve emergency plans and procedures for continued operation during undesirable events and ensure that operators are trained to implement these contingency plans.

- Modify the physical system—improve control centers and protective devices, increase redundancy of key equipment, and increase reserve margins.

Measures to Speed Recovery

- Conduct contingency planning for restoration of service, including identification of potential spare parts and resolution of legal uncertainties.

- Clarify the legal and institutional framework for sharing reserve equipment.

- Stockpile critical equipment (e.g., transformers, pumps, compressors, regulators) or any specialized materials (e.g., cables, pipe sections) needed to manufacture critical equipment or make repairs.

- Assure availability of adequate transportation for stockpiles of very heavy equipment by maintaining a database of rail and barge equipment and adapting Schnabel railcars to fit all needed types of large pieces of equipment, if necessary.

- Monitor domestic manufacturing capability to assure adequate repair and manufacture of key equipment in times of emergency.

- Investigate mutual aid agreements with vendors, industry associations, or large near-by energy companies.

- Establish backup arrangements with contractors for emergency services and other emergency support.

General Mitigation Measures to Reduce Vulnerability

- Emphasize inherently less vulnerable technologies and designs when practical, such as using standardized equipment.

- Move toward an inherently less vulnerable bulk energy system (e.g., smaller generators near loads, local storage) as new installations are planned and constructed.

As indicated earlier, local governments should coordinate energy facility activities related to risk management. The following questions can help guide local and state governments through the risk management process.

Local and State Government's Role in the Risk Management Process
☐ Has the local or state government identified any critical issues or vulnerabilities regarding its energy infrastructure?
☐ If the local or state government has identified critical issues, what are they and why are they critical?
☐ Has the local or state government developed plans to counter these vulnerabilities?
☐ Has the local or state government coordinated information with other local energy facilities, local law enforcement agencies, and others concerning these vulnerabilities?

4 Sources

A number of sources were consulted in preparing this checklist. The major sources of the materials used are listed below.

Analytical Risk Management: A Systems Approach to Decision Making, DOE's Nonproliferation and National Security Institute (NNSI)

> The NNSI conducted a two-day training course at DOE Headquarters on November 1 and 2, 2001. In addition to NNSI, representatives from Texas and other federal agencies participated in the training course. Feedback from this pilot course and from state visits will be used to develop training for states interested in this approach.

Summary Information from the Vulnerability and Risk Analysis Program (VRAP) of DOE's Office of Critical Infrastructure Protection

> DOE's Vulnerability Survey and Analysis Program has been working with the national energy sector to develop the capability required for assuring the security of our nation's energy infrastructures. Many initial best practices have been assembled as part of DOE's initiative to help energy sector organizations identify and understand the threats to and vulnerabilities of their infrastructures. Many of these best practices are included within this checklist.

Assessment and Strategy Development Tool Kit of the Fiscal Year 1999 State Domestic Preparedness Equipment Program, Office of State and Local Domestic Preparedness Support, Office of Justice Programs (OJP), U.S. Department of Justice

> This easy-to-use risk assessment tool was developed for OJP specifically to assist users at many jurisdictional levels in responding to weapons of mass destruction terrorism. The OJP tool kit asks for information in specific formats to help determine priorities for grants needed to purchase equipment. Texas has used this tool, or a version similar to it, for a statewide terrorism assessment.

Subject-Matter Expert Input Readily Available to DOE's Office of Energy Assurance

> This source of information includes individuals with experience in conducting and documenting vulnerability analyses and risk assessments, individuals with experience in responding to energy sector emergencies, and individuals currently working to build new models and methods for assessment of large, complex infrastructures.

Appendix: Key Definitions and Nomenclature

Key Definitions

Adversary: An individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to the U.S. government or its assets. Adversaries include intelligence services of host nations, political or terrorist groups, criminals, and private interests.

Asset: Any person, equipment, material, information, installation, or activity that has a positive value to an organization or facility. The asset also may have value to an adversary, although the nature and magnitude of those values may differ.

Cost-Benefit Analysis: Part of the management decision-making process in which the costs and benefits of each alternative are compared and the most appropriate alternative is selected.

Mitigation or Protective Measure: An action taken or a physical entity used to reduce or eliminate one or more vulnerabilities. The cost of a possible mitigation measure may be monetary or non-monetary (e.g., reduced operating efficiency, adverse publicity, unfavorable working conditions, and political consequences).

Impact: The amount of loss or damage that can be expected. The impact may be influenced by time or other factors.

Risk: The potential for damage or loss of an asset. The level of risk is a condition of two factors:

- the value placed on the asset by its owner and the consequence, impact, or adverse effect of loss or change to the asset and
- the likelihood that a specific vulnerability will be exploited by a particular threat.

Risk Assessment: The process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management: The process of selecting and implementing security protective measures to achieve an acceptable level of risk at an acceptable cost.

Threat: Any indication, circumstance, or incident with the potential to cause the loss of or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to U.S. interests. Threat categories include insider, terrorist, intelligence service, environmental, criminal, and military.

Undesirable Event: Any incident with the potential to cause the loss of or damage to an asset. Undesirable events can be due to actions such as theft, compromise, destruction, sabotage, assault, assassination, and kidnapping or due to occurrences such as non-availability or impaired operation of an asset.

Vulnerability: Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from the following:

- building characteristics;
- equipment properties;
- personal behavior;
- locations of people, equipment, and buildings; and
- operational and personnel practices.

Nomenclature

ANSER	service provided by Analytical Services, Inc.
DOE	Department of Energy
EMS	energy management system
FBI	Federal Bureau of Investigation
HVAC	heating, ventilation, and air conditioning
IT	information technology
NIPC	National Infrastructure Protection Center
NNSI	Nonproliferation and National Security Institute
OEA	Office of Energy Assurance
OJP	Office of Justice Programs
OPSEC	operations security
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
UPS	uninterruptible power supply
VRAP	Vulnerability and Risk Analysis Program