Federal Energy Management Program

Leading by example, saving energy and taxpayer dollars in federal facilities

Performing Energy Security Assessments —

A How-To Guide for Federal Facility Managers

U.S. Department of Energy
Energy Efficiency and Renewable Energy
Bringing you a prosperous future where energy is clean, abundant, reliable, and affordable

Contents

EXECUTIVE SUMMARY

As a facility or energy manager at a federal facility, you may find it necessary to conduct an energy security assessment at your site to identify threats to your energy supply and ensure that a reliable energy supply is always available to carry out critical functions. This guide presents a methodologies and approaches for conducting energy security assessments at federal facilities. The guide draws from best practices and lessons learned from experience gained by Oak Ridge National Laboratory (ORNL) in 2004 when it helped 16 Southeast Regional Office Army installations develop their energy security plans.

This guide is designed to be flexible enough to accommodate the needs of the broad spectrum of federal installations that will use it. The best practices and lessons learned that are summarized in this executive summary are applicable to the following:

- Initiation of the energy security assessment process
- Vulnerability assessment
- Energy preparedness and operations plan
- Remedial action plan
- Management and implementation

Getting Started

- Assign an energy security manager to lead the energy security program at the site.
- Create an energy security planning board to provide site expertise and facility data and to make decisions. (This may not be applicable to small sites.)
- Consider the site's mission and function as a guide during the assessment.
- Understand the energy security assessment program process and the process flow.
- Sponsor a kickoff meeting to establish ground rules, orient analysts or consultants, and foster cooperation between all site organizations. (This may not be applicable to small sites.)
- Effectively anticipate and manage potential delays as described in Sect. 2.6.

Vulnerability Assessment

- Create or update energy system descriptions, including energy feeds/deliveries to the site.
- Identify critical facilities and associated loads based strictly on the site's mission and/or function.
- Identify critical energy requirements from on-site sources and off-site energy feeds.
- Identify all significant potential threats from natural phenomena, fires, accidents, equipment failure, and intentional causes.
- Perform a probabilistic vulnerability analysis for all identified threat scenarios.
- Derive both a best estimate and a maximum estimate of impact duration for all viable threat scenarios while considering the availability of repair crews in each case.
- Based on the results of the probabilistic vulnerability analysis, list unacceptable risks to be addressed by the remedial action plan.

Energy Preparedness and Operations Plan

- Brainstorm alternative plans for continued operation during energy outages.
- Prepare lists of personnel contact information for energy emergencies.
- Know what functional agreements exist for emergency support.
- Inventory and manage emergency generators, both fixed and portable.
- Describe the training plan for staff operations during an energy emergency.
- Review prior and current energy-related construction projects for the site.

Remedial Action Plan

- Brainstorm plans for remedial actions to address unacceptable risks while relying on site experts, consultants, facility surveys, and/or new technologies. (At small facilities, site experts may make these determinations.)
- Carry over projects identified during prior years if the need and priority remain.
- Prepare a remedial action plan that includes top-priority and/or budgeted projects.
- Explore alternative means for funding remediation projects, such as the following:
  - Appropriations/military construction
  - Energy savings performance contracts
  - Utility energy service contracts
  - Public-private energy ventures
  - Enhanced-use lease
  - Utility privatization

Other Considerations

- Determine whether to use consultants and consider their advantages in the vulnerability analysis process and the creation of effective and synergistic remediation projects. (This may not be applicable to small sites.)
- Carefully develop remediation plans to support the site's mission and function.
- Maintain ongoing reviews and prepare updates of the energy security plan.
- Do not underestimate the critical importance of information security throughout the assessment process.

Performing Energy Security Assessments — A How-To Guide for Federal Facility Managers

1. INTRODUCTION

Energy security is one component of general physical security that has recently gained great importance for many commercial, industrial, and government facilities. This guide describes best practices for developing an energy security assessment and threat mitigation program to help ensure that reliable energy is available to maintain critical functions at federal facilities.

Today, building owners and facility managers have a responsibility to consider a broad array of potential threats and incident scenarios. Such an evaluation ultimately leads to the complex task of identifying and choosing which hazards to guard against. These hazards may have natural or man-made causes, the latter of which are highly unpredictable. An underlying process or methodology is essential to comprehensively and intelligently address all elements of energy security analysis.

This best practices guide describes a recommended process for preparing the following sections of a facility's energy security plan:

- vulnerability assessments
- energy preparedness and operations plans
- remedial action plans

This information is supplemented with practical considerations for implementing an energy security assessment program and numerous lessons learned that should benefit initial assessments. Finally, a template for an energy security plan is provided in Appendix A. This template can be used for large installations or adapted as needed for smaller sites or specialized applications.

1.1 Facilities to be Assessed

A few examples of facilities that need energy security assessments are some Department of Energy (DOE) and Department of Defense (DoD) facilities, government offices with essential missions, defense-related installations, and command and control facilities.

The 12 critical sectors that are cited by government experts (Office of the President 2003) are:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Postal and Shipping

In addition, it is important to preserve critical resources such as national monuments and icons, nuclear power plants, dams, government facilities, and key commercial assets. Some federal sites, including the defense industrial base, have many facilities owned and operated by DoD. The Postal Service is separately identified.

A few examples of non-governmental facilities that may similarly benefit from an energy security plan are key energy infrastructure sites such as oil refineries, electrical generation plants, fossil fuel plants, munitions manufacturers, communications centers, and key financial centers. In fact, a truly comprehensive listing would be all but impossible to develop.

Energy security assessment programs may pertain to any type of building, facility, base, or installation. In most cases, this guide will refer to them simply as "sites," since this term does not imply any particular size or function. Terms other than "site" will be used in specific cases as needed.

The following section of this guide describe

- the activities and best practices for beginning the assessment process and in periodic updates,
- the tasks necessary to evaluate the vulnerabilities of energy sources,
- the activities necessary to ensure that the site has adequately addressed energy preparedness through planning and the documentation of critical information and that an operations plan is in place
- the process for developing a remedial action plan, and
- issues to consider in conducting an energy security assessment.

2. BEGINNING THE ENERGY SECURITY ASSESSMENT PROCESS

The energy security assessment process is intended to develop an energy security plan, which comprises a vulnerability assessment, an energy preparedness and operations plan, and a remedial action plan. This section describes the activities and best practices to follow in beginning the assessment process and possibly during periodic updates.

2.1 Assign an Energy Security Manager

Every site should designate an energy security manager to ensure that there is a person responsible for leading the energy security program and meeting program milestones and goals. Depending on the size of the site and the extent of peripheral activities such as managing remediation, this may be a near-full-time job. The energy security program should be approved by the site manager. The energy security manager typically communicates with groups such as the energy security planning board (see Sect. 2.3), site engineers, physical security personnel, fire protection personnel, electric power distribution and fuel delivery personnel, site managers, and off-site entities such as the electricity and fuel providers. The energy security manager must ensure that the process moves along on schedule and that the board adheres to procedures.

Energy security programs for large and/or complex installations may require the assistance of consultants to perform analyses and prepare documentation. The energy security manager hires the consultants and works closely with them to ensure that they obtain the information they need in a timely manner. He or she also ensures that the documentation accurately reflects the energy infrastructure and dynamics of the site relative to energy types, usage, capacities, storage, critical facilities, critical sources of primary and backup power, types of emergency situations, contingency plans and capabilities, and realistic threat scenarios.

The energy security manager also ensures that the energy security plan for the site is updated yearly or as determined by the approved site plan.

2.2 Define the Mission of the Installation

It is essential that the mission or the critical functions of the site are precisely defined at the beginning of any initial energy security program or periodic update. Planners cannot identify critical facilities and identify unacceptable risks at the site without knowing the mission. Likewise, an understanding of the mission is necessary to fully analyze threat scenarios that may adversely affect critical facilities.

Carefully evaluate the mission, whether well established or recently redefined, to determine whether an energy security assessment is even required and, if one is pursued, whether the scope of the assessment is appropriate. For instance, a certain portion of a military base may need to be added to or dropped from the assessment based on changes to the mission. Also, a well-established and funded expansion of the mission that includes the construction of a new facility might benefit greatly from the inclusion of the new facility in the assessment. Ideally, this process could be designed to feed hazard mitigation recommendations to the facility planners and designers for immediate incorporation into design changes that can result in considerable cost savings.

2.3 Create an Energy Security Planning Board

An energy security planning board is useful for larger installations or when deemed necessary by either site management or the energy security manager. The U.S. Army's DEPPM 92-1 recommends that each DoD installation create such a board, since "the utilization of an [energy security planning board], with the installation commander or designated representative as chair and representatives from each tenant/command, will help assure a coordinated planning and recovery effort."

The primary duties/functions of the board are

- providing an integrated site knowledge base that includes fire protection, physical security, operations, and energy security,
- making decisions based on the board's site expertise,
- obtaining required energy-related site data to support the process (see Sect. 3.4, "Analyzing Potential Threats), and
- establishing program schedules and plans for updates.

Vulnerability assessment engineering consultants could attend a meeting of the board to obtain essential information. Monthly meetings during the preparation of the energy security plan are recommended.

As indicated in Sect. 2.1, the energy security manager must ensure that the board adheres to procedures.

2.4 Know the Process and Process Flow

The energy security assessment program is designed to produce an energy security plan that defines and technically justifies projects that, if implemented, should significantly improve energy security at the site. Figure 1 depicts the general functional flow for

the energy security assessment program. On the left side of the diagram, the energy security manager and the site personnel interact to a high degree to produce the information and decisions necessary to support each activity. The board, if one exists, is also active in this information-gathering and decision-making process.

The right side of Figure 1 shows the three main processes that must be undertaken to produce an energy security plan: the vulnerability assessment, development of an energy preparedness and operations plan, and creation of the remedial action plan. In the end, the process not only recommends projects to improve energy security, but also documents (as indicated by a separate box in the figure) many types of information that are useful both to support the process and to provide a quick reference during energy disruptions. Primary types of documentation include alternate means of maintaining critical functions, emergency personnel contacts, personnel recall procedures, emergency support agreements, mutual aid agreements, a listing of generators, the training plan, and energy-related construction projects.

Examples of a detailed breakdown of each element of the energy security plan are provided in the Sects. 3, 4, and 5 of this guide and in the template in Appendix A.

2.5 Consider Sponsoring a Kickoff Meeting

At medium to large installations, an initial meeting of the energy security manager and the energy security planning board may be very useful for establishing the ground rules of the program and describing how it will be managed and implemented. The meeting is an excellent opportunity for scheduling the energy security plan update and future meetings of the board. It is important to establish an understanding of the goals and the methodology for accomplishing the goals.

The success of the kickoff meeting hinges strongly on whether the right people attend. The energy security manager should determine which individuals and organizations should be included to provide answers and help in making decisions such as the designation of critical facilities. Site management, funding sponsors, and consultants should be encouraged to attend as well. To ensure that the needed people attend, emphasize the importance of the meeting so that staff will schedule their other commitments around it.

2.6 Anticipate Delays and Barriers

How well the energy security assessment process progresses depends on many factors, such as the type of mission or critical function of the site, the size and complexity of the site, available funding for energy security, the capabilities of the energy security manager, the effectiveness of the energy security planning board, the site management's interest, and other factors and intangibles.

During the initial energy security assessment for several U.S. Army installations in 2004, a variety of approaches were tried. These ranged from a determined attempt at one small site to complete the energy security plan during a one-day meeting to an approximately six-month process at a much larger site that was all but stalled during a third of the period. Neither of these extreme cases was necessarily inappropriate or without basis at the particular site; however, a measured and methodical approach with an emphasis on good communication is a necessary best practice.

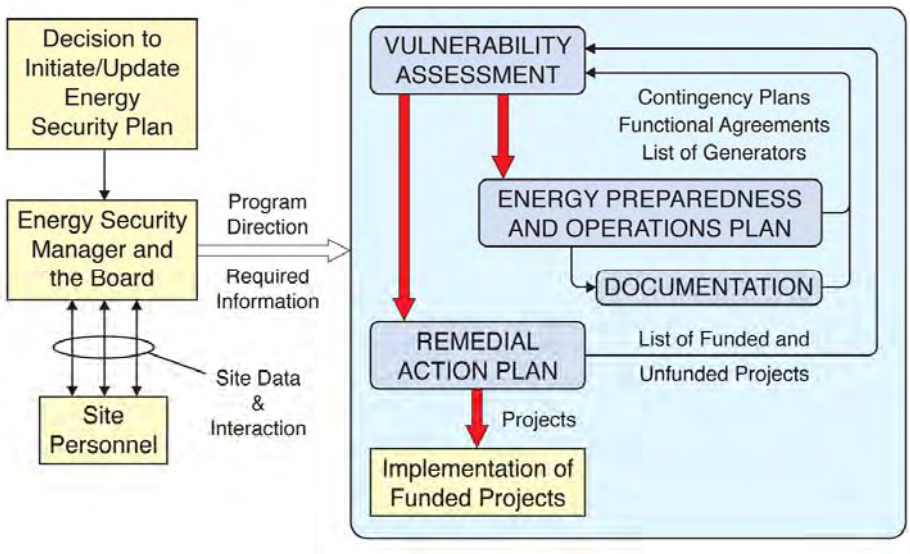

Figure 1. Energy security program flow diagram.

Lessons Learned: Assuring Information Security

The most significant barrier encountered during the 2004 program was related to site security (see Sect. 6.5). At one large garrison the energy security planning board, after considering the type of information that was being requested for completion of the energy security plan, raised a significant security issue. The board asserted that if the collected information pointing to the vulnerabilities of their energy sources and general physical security were to be published and sent outside the base, the risk of its falling into the wrong hands would be unacceptable. The argument that security cannot be improved unless vulnerabilities are known and assessed did not sway the board. Assurances that the vulnerability assessment and threat mitigation portions would be classified also were not helpful. The energy security manager believed that the board's concerns could be assuaged if board members were assured that the energy security plan would never be transmitted off-site. The manager also initiated a process to have the chief of staff issue a directive making the information collection process mandatory.

The directive issued by the chief of staff stated, in part:

- *[The] Energy Security [Planning] Board will produce a plan that identifies vulnerabilities, of the mission and facilities, to energy disruptions in order to take action to eliminate critical energy support vulnerabilities. The Energy Security Plan will be completed and presented to HQ, IMA by 30 September 2004.*
- *[The energy security manager] will: (1) establish and enforce milestones necessary to meet the 30 September 2004 suspense; (2) in conjunction with PSBC, conduct energy vulnerability analyses; (3) conduct liaison with public utilities and other off-base service providers to ensure critical base missions are recognized in the service restoration plans of those providers; and (4) … develop and execute remedial action plans to remove unacceptable energy security risks.*
- *Tenant Commands will: (1) provide a representative to the Energy Security [Planning] Board; (2) provide their critical energy requirements (including electrical and fuel) and backup generator capability to [the energy security manager]; and (3) establish and maintain a technically accurate data base of its portable emergency generators.*

In time, the energy security manager's actions proved effective in resuming the information-collection process.

Lessons Learned: Selection of Critical Facilities

The second most significant barrier encountered in 2004 related to the selection process that identifies critical facilities at the site. This barrier is most likely to exist at medium to large sites, and the use of an energy security planning board does not necessarily affect the likelihood that this barrier will become an issue. This barrier is fully discussed in Sect. 3.2.

3. CONDUCTING A VULNERABILITY ASSESSMENT

This section discusses tasks necessary for evaluating the vulnerabilities of energy supplies such as electricity, natural gas, and fuel oil. A comprehensive evaluation for a large site can be technically demanding because of the interdependencies between the different types of energy. For instance, electricity is vulnerable to many elements of the system infra-structure. Among other requirements, an optimal, stable electrical system may need (1) transportation available (roads or rails must be free to deliver fuel), (2) oil as a fuel and a lubricant, (3) communications for supervisory control and data acquisition (SCADA) systems, and (4) natural gas as fuel for electricity generation and heating. It is necessary to see how each element interacts with others, creating a tightly woven set of interdependencies that must be addressed to maximize the security of the system.

An energy security plan comprises a vulnerability assessment, an energy preparedness and operations plan, and a remedial action plan. The vulnerability assessment is the most technically involved of the three.

3.1 Identify Critical Sources of Energy

Critical sources of energy and primary energy storage facilities must be identified in detail before proceeding with the vulnerability assessment. The following subsections describe this task and suggest best practices.

3.1.1 Describe on-site and off-site electrical systems

The electrical distribution systems and the overall source of electricity are generally the most important energy systems for energy security and are certainly the most complex. Place the greatest emphasis on the on-site distribution system and, if applicable, any on-site central generation system and on-site substation(s). Fully describe any system providing added flexibility, such as alternate feeds, systems to switch off noncritical loads, and power monitoring and control systems. Characterize the general state of maintenance, as well as any known system weaknesses. Describe current or planned system upgrades and the reasons for the upgrades (see Figure 2).

Although the security of the water supply system is outside the scope of an energy security assessment, the energy supply to the water pumps may be deemed critical to the mission or function of the site. In such a case, include the pumps as a critical facility.

Describe the off-site electrical system in terms of electrical feeds to the site and what off-site substations and switching stations directly supply power. The grid system in the local community is likely to be very complex; therefore, take care to avoid describing the off-site system beyond what is actually known. Electricity providers often will not provide details on sensitive information such as which substation-to-substation ties are important or likely to be used, where their greatest system vulnerabilities are, or what emergency contingency plans may be used. (Also, contingency plans are generally limited by changing load levels, fixed equipment capacity ratings, and the details of particular grid-related upsets.) Historical records that reflect the robustness of the off-site system and the duration of outages relative to different events may be the most pertinent kind of information that can be documented.

3.1.2 Describe deliveries and storage of all fossil fuels

Many critical sites depend on the availability of diesel fuel, propane, and/or natural gas. Coal is also used at some sites to fuel steam generators. Describe each fossil fuel type in use at a site in terms of its applications and whether a dual fuel capability exists. Describe transportation, piping, and storage of fossil fuels in terms of logistics and general reliability. Provide an overview of the physical security of storage (see Figure 3) and distribution systems. Mobility fuels and other special, mission-related fuels are generally outside the scope of the site vulnerability assessment unless required by site management.

3.1.3 Define thermal requirements and applications

Evaluate supplies and storage of hot water and steam, including distribution, to determine how critical each is to supporting the mission and critical functions of the site. Of course, facility heating and general cleaning are the most common uses of these thermal supplies. The vulnerability of steam lines depends a great deal on whether they are routed overhead or underground; therefore, identify the general routing of steam lines.

Figure 2. Use of old wooden poles and new hurricane-grade concrete poles at Fort Buchanan, Puerto Rico.

3.2 Identify Critical Facilities Based on Mission Accomplishment

This section provides information that helps identify critical facilities for use in preparing Table 2-1 in the energy security plan

(Appendix A). The appropriate selection of critical facilities is of utmost importance, since the list of critical facilities will serve as the foundation for the rest of the energy security plan. The determination of whether a particular facility is critical hinges on whether the facility is essential to the mission or the function of the site. The energy security manager and energy security planning board must consider for each facility the consequences of interrupting any supply of energy. If the mission would suffer significantly, the facility is probably critical.

At this stage in the process, consider only how critical the function of the facility is, not its vulnerability or invulnerability. For example, in identifying critical facilities it is irrelevant whether the facility has a reliable backup source of energy or dual fuel capability, or whether there is another facility to which the activity/function could be immediately transferred.

There may be gray areas in this decision process. However, maintain high standards for defining a critical facility rather than including facilities "just to be safe" or to avoid making a decision. Some Army sites found that the existing list of mission-essential vulnerability areas (MEVAs) and "high-risk targets" were useful in determining critical facilities.

In medium to large installations, there may be building managers or tenants who have preconceived ideas about the selection process. They may imagine that if their facility is not selected as a critical facility, it will be forever bypassed in funding for upgrades. Such attitudes are a good example of why determining critical facilities should be a methodical and consistent process. The energy security manager should take steps to address this misconception if it is prevalent, emphasizing that the process of selecting critical facilities and the subsequent assessment process are concerned exclusively with energy security and energy-related remediation plans.

For each critical facility, the energy security manager should obtain estimates from tenants/building managers of the levels of energy required to support their critical facilities. If energy usage can be easily trimmed to only what is required to support critical loads, then the estimate should be for that reduced energy requirement. Of course, some facilities' emergency energy requirement may be somewhat elevated, depending on the scope of their emergency operations.

3.3 Make Note of Energy Sources On Site and Off Site

Given that the critical energy requirements are now established for each of the critical facilities, the next steps are to (1) identify primary energy sources, (2) list the rating and capacities of those sources, (3) identify backup energy sources, and (4) identify critical *off-site* energy systems that are essential to the installation for normal and emergency operations. This information and contacts for responsible parties are entered into Table 2-2 (on-site energy sources) and Table 2-3 (key off-site energy systems/feeds) in Appendix A.

This step completes the energy source profile up to the point where a backup source of energy may fail or become unavailable. The planned response to this important issue will be addressed later (in Table 3-1 of the energy security plan).

3.4 Analyze Potential Threats

This section provides information on analyzing significant potential threats to a site that will be listed in Table 2-4 in the energy plan (Appendix A).

Figure 3. Fuel storage security must be assessed relative to all viable threats.

The threats may be due to natural phenomena, equipment failure, accidents, or intentional threats by individuals desiring to cause an energy interruption.

Following the identification of critical facilities and critical sources of energy, the potential for disruption of critical energy supplies must be assessed in detail so that estimates of probabilities can be made. This will involve analyzing a number of possible threat-related scenarios. Then the analyst must estimate the impact of each threat on each type or source of energy. Knowing the probability and the potential impact will enable the analyst to consider relative risk and, in this way, form a good basis for recommending risk remediation.

3.4.1 Consider the threat categories

This section considers the type of threat scenarios that may be considered in a probabilistic vulnerability analysis. Section 3.4.2, "Perform Probabilistic Vulnerability Analysis," provides a discussion and an overview of the analyses themselves.

Natural phenomena

A number of natural phenomena can pose site-specific threats to energy supplies:

- Earthquakes
- Floods
- Hurricanes
- Tornados
- Extreme heat
- Ice storms

Depending on the site's location, other initiators (e.g., volcanic activity or tidal waves) may have to be considered. Published flood event data for various areas of the country are normally all-inclusive and not segregated according to the cause. Thus, flood data will include events from both hurricanes and other storms. Since all flooding is considered separately, hurricane analysis should be for winds only. Tornados should be considered apart from hurricanes (see Figure 4), except that hurricane-spawned tornadoes should be considered together with hurricanes.

Extreme heat during the summer months may apply to most areas but not to certain coastal areas or islands if climatological data indicate that temperatures are always moderated by the large water masses and high humidity. Ice storms are notorious for causing long-duration electrical outages over a wide area; however, their likelihood and range of severity are dependent upon site location.

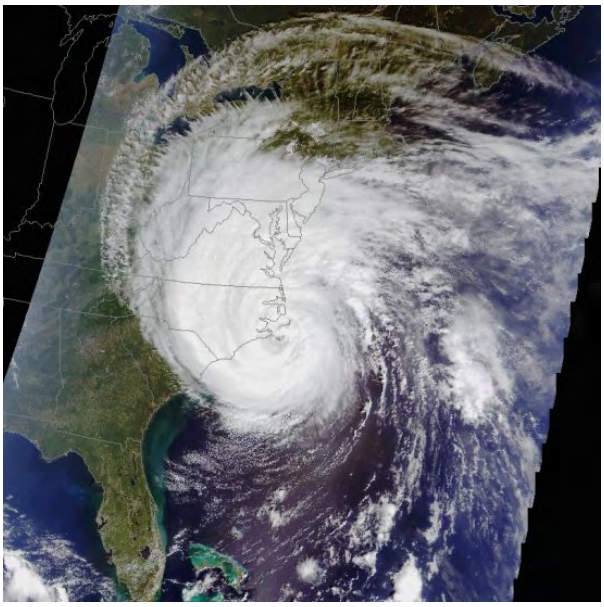

Figure 4. Compared with tornados, hurricanes have very widespread effects with winds of much longer duration.

Site-specific threats

Site-specific threats to energy supplies can also be the result of the following accident- and equipment-failure-related initiators:

- Fire
- Accident
- Mechanical failure
- Electrical failure

Fires can be both human- and equipment-related. Accidents, as distinguished from fires, arise from human activities that have gone awry, resulting in an inadvertent, adverse physical impact to energy storage and/or distribution systems such that physical damage and a disruption occur. Accidents can occur during facility modifications, construction, material handling, energy system operation, transportation, and frequent flight operations. Human error frequently plays a part in accidents.

Mechanical failure, in the context of energy security planning, refers to an equipment failure, most likely in an energy-related system, that may cause an energy disruption. Of greater significance and frequency is electrical failure (electrical or electronic failure), possibly in an energy-related control system, that may cause disruptions. In threat analysis it may be helpful to combine the mechanical and electrical failure categories into one.

Intentional threats

In addition to the unintentional threat initiators discussed above, the following intentional initiators should be considered:

- Labor strikes or contract default
- Sabotage, terrorism, or riots
- Arson and vandalism
- Cyber attacks on computers and control systems

Labor-related energy disruptions are primarily nonviolent; a service such as fuel delivery is simply interrupted over an extended period. Sabotage, terrorism, or riots are generally distinguished from arson and vandalism by the level of intent, planning, determination, goal, severity, and/or number of people involved. Arson and vandalism are generally pursued in a more casual, spontaneous, and random way, often without any resolute or compelling purpose or goal. Cyber attacks can be viewed as mostly random, although incidents may increase at government and military sites during wartime.

3.4.2 Perform probabilistic vulnerability analysis

It is beyond the scope of this best practices guide to describe in detail how a probabilistic vulnerability analysis should be performed; however, this section provides an overview of the process, with some guidelines that can be used in reviewing a vulnerability analysis for completeness and overall quality. Probability analysis is a well-established process, and for additional assistance many consultants are available to provide help.

Some sites may have records of accidents, fires, weather-related power outages, and other threat-related events. Such data are definitely preferable to generic, published probability estimates and can be very useful in a vulnerability analysis because they refer to actual events at the site. In some cases, data for a certain type of event may be scarce or nonexistent, which may call for tracking the data as an action item or remedial action for site personnel in future years (see Sect. 4.1, "Define a Plan B for Continuing Operations").

If program funding does not allow a comprehensive analysis, a strictly qualitative approach may be necessary, perhaps based on little more than judgments by the energy security manager and the planning board as to whether the event has a high, medium, or low likelihood at their site.

In the case of threat scenarios based on natural phenomena, consult natural phenomena data for the general site location. The U.S. government and many states post useful data on Internet sites [such as those cited in Refs. 2–8] that can be easily found using key words. These data may allow the analyst to create a quantitative estimation of the probability of the event at the site without excessive time and effort. Even very general statistical data can be useful (see Figure 5).

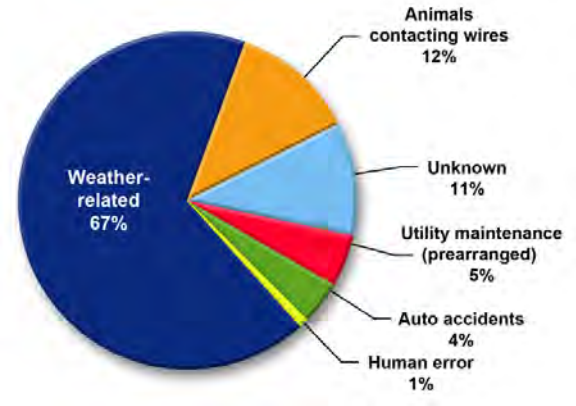

Figure 5. Primary reasons for power outages. Source: Edison Electric Institute, 1999 Reliability Report.

A threat scenario may be considered to be "very low" if the probability of occurrence is $\leq 1 \times 10^{-4}$ events per year and "low" if the probability of occurrence is $\leq 1 \times 10^{-3}$ events per year. These correspond to an event occurring no more than once in 10,000 years and 1,000 years, respectively. As a best practice, it is recommended that $\leq 1 \times 10^{-4}$ events per year be considered "insignificant."

In the case of accidents and equipment failures, event probabilities can depend on numerous factors. For the vulnerability analysis, actual site accident data are preferred; industrial accident data are a less-preferred second choice. (The applicability of generic industrial data, even from highly respected sources, may depend on many subtle nuances related to how the data was collected and processed.)

For equipment failures (primarily failures of electrical equipment), site data are again highly preferred, since the equipment failure frequency at the site is a function of the general equipment quality and the frequency and quality of maintenance at the site. If the frequency of site equipment failure cannot be estimated, the analyst will have to rely on industrial data from sources such as the IEEE [9–10]. The IEEE itself asserts that site-specific data are always to be preferred [10].

In the case of intentional events, estimating a quantitative probability for a given scenario is no longer possible. If U.S. government homeland security experts freely admit they cannot predict the likelihood of specific threats, it is not likely that a private consultant or a site expert will be

any more successful in this endeavor. In assessing the potential for labor disputes to cause an energy outage, the analyst should review related news published by the local community that supplies the site with its energy needs.

The probability of sabotage, terrorism, or riots will be greater for sites that are very well known, symbolic, soft targets, important to the economy, active, and well populated. Planners and perpetrators of these types of activities generally consider what potential global news impact may exist in selecting a particular target. It is important to energy security that some of the most enticing sites for saboteurs and terrorists are those in the energy production industry, such as nuclear plants and oil refineries. This may have implications for sites whose operations depend on these types of potential targets.

Countering these considerations, the sheer size and economic vitality of the United States results in a large number of attractive targets; the large number of targets tends to dilute the potential threat at any one site. Hence, the assignment of a "low" threat probability will be common for many sites, including those that have critical functions and/or important missions.

3.4.3 Estimate the duration of impact

Each threat scenario requires an estimation of a corresponding impact. In determining overall risk to a site, the expected and maximum duration of an impact or energy disruption is as important to consider as the probability of the threat scenario.

If, on an otherwise uneventful day, a diseased tree falls on an electric line causing a fault, a disruption may last 2 hours. If the same tree falls during a severe ice storm when widespread outages are occurring over a multi-county area, the same fault may not be cleared for 20 hours. This order-of-magnitude increase in duration of impact is a result of the scarcity of repair crews during a widespread emergency. For the same reason, the impact duration of a tornado that has damaged a site will generally not be as severe as that of a hurricane that has damaged the site and also much of the state. Ice storms and hurricanes, both of which cause widespread damage, have caused energy outages lasting several weeks on many occasions in the United States during the last 50 years. Tornados, floods, accidents, and electrical equipment failures generally do not have the same duration of impact. Nevertheless, in some cases tornados have caused extended power outages, as suggested in Figure 6.

The analyst can estimate expected and maximum impact durations for threat scenarios by considering the following:

- How widespread the damage may be on the site and environs
- How difficult it will be to repair damage, restore fuel supply, etc.
- What site experts say about the duration of past interruptions
- What off-site experts estimate for restoration in each type of scenario
- The level of system redundancy, number of tie lines, and spare power
- The availability of replacement equipment that may be scarce
- The temporary work-around solutions available for power restoration

The determination of a best-guess estimate or the *expected* duration of an energy outage is useful for determining the relative risk of each scenario. The determination of the *maximum* estimate of the duration is useful for flagging potential problem areas that may or may not represent an unacceptable risk.

Care should be used in considering risk based on maximum impact. The estimated scenario probabilities and the maximum duration of impact generally do not correspond with each other. The

Figure 6. Tornado strikes on transmission towers: (a) May 1998 Muskegon wind storm topples five 345-kV towers; (b) November 2002 tornado strikes 500-kV tower in Tennessee; (c) June 1999 tornado damage in Illinois.

longest-duration or worst-case scenario almost always has a significantly lower probability than that for other scenarios relating to the same general threat. Strictly speaking, the probability needs to be adjusted downward before determining risk based on a maximum-duration scenario. If an analyst cannot derive an adjusted probability, it is best to consider the estimate of maximum duration itself as an indication of the worst-case scenario. However, a caveat applies: Remedial actions should never be based on an estimate of maximum impact by itself; only risk comparisons should be used.

3.5 List Unacceptable Risks

An unacceptable risk is defined as an estimate that energy supply interruptions are both reasonably likely and cannot be sufficiently mitigated so that affected organizations can perform their critical missions. This section discusses the determination of threat scenarios having unacceptable risks and provides information that will help in identifying unacceptable risks and preparing Table 2-5 in Appendix A. Only scenarios deemed to have an unacceptable risk are shown in the table. (The remedial action process, discussed in Sect. 5, identifies risk mitigation actions for each unacceptable risk.)

At this stage in the process, scenarios that are determined to have an unacceptable risk are listed, along with a short description of remedial actions that would be effective in reducing the risk. This represents a meshing of the final task of the probabilistic vulnerability analysis/impact evaluation and the first step of the remedial action process. It is essential that the vulnerability analysis findings feed into the remedial action process and the proposed corrective actions on a scenario-by-scenario basis whenever the risk is unacceptable.

Consider the probabilistic vulnerability analysis and the best estimate of impact duration together in establishing a risk for each threat scenario. To do this, the analyst may rely on engineering judgment. Ideally, a consistent methodology would be used for assessing the risk of each scenario; however, the methodology would have to accommodate variations in data, such as quantified probabilities for some scenarios and qualitative estimates for others. As discussed previously, variations in a scenario cause variations in the scenario impact. Also, the estimated impact durations may be a narrow range or a broad range. Thus, the process of identifying unacceptable risks and remediation is not a mathematical science but a combination of qualitative evaluation and engineering judgment.

Note that risk is not explicitly denoted but, instead, is inferred from the likelihood of the threat or scenario and the longevity of the impact duration. A high-probability, short-duration event may have an acceptable risk since workarounds can often be implemented on a short-term basis. Conversely, a low-probability, long-duration event may also have an acceptable risk since the remediation cost may not be justified for events that are estimated to occur once every few thousand years.

4. ESTABLISHING THE ENERGY PREPAREDNESS AND OPERATIONS PLAN

This section addresses activities necessary to ensure that the site has adequately addressed energy preparedness through careful planning exercises and the documentation of critical information such as emergency personnel contacts and generator testing. It also ensures that an operations plan is in place that specifies which organizations may be needed in an energy emergency and what their function should be.

4.1 Define a "Plan B" for Continuing Operations

This section provides information that will help identify energy supply workarounds, which is needed in preparing Table 3-1 in Appendix A. A key to energy preparedness is the process of thinking through what actions should be taken in the event of a critical energy outage. At this stage, the analyst should look beyond the obvious (e.g., start the emergency generator) to what actions could be taken if the primary energy source and any secondary source of marginal or indeterminate reliability is lost. The reliability of generators (Figure 7) is generally indeterminate, since they are not tested under actual load conditions.

Site experts should consider energy outages and identify innovative means of supporting continued operations. This may entail finding other energy sources that could be transported to the facility, or moving operations to another facility. This process, if well thought out, can be one of the most beneficial products of the energy security plan and may greatly enhance energy emergency responsiveness.

4.2 Identify Contact Information for Emergency Resources

This section provides personnel contact information needed to prepare Table 3-2, Table 3-3, and Table 3-7 in Appendix A. It describes the full

Figure 7. The reliability of building generators is less than ideal for the purposes of energy security.

range of information resources that should be prepared and updated as needed or, at a minimum, with each update of the energy preparedness and operations plan.

Three categories of information resources must be prepared:

- *Emergency contact personnel*—Prepare a tabular listing of emergency contact personnel to serve as a convenient reference during energy outages. Include names, phone numbers, and other communication channels for key site personnel, including administrative, security, and public affairs staff, the fire chief, and others. How extensive the administrative and functional listings are will depend largely on the size of the site. In addition to site personnel, list other DoD, federal, intelligence, and state and local emergency contacts. This listing will also be determined by the nature of the site, its mission, its function, and other factors.
- *Staff recall list*—An energy outage may necessitate a measured staffing-up in order to effectively resolve the problem. Prepare a personnel recall procedure and a recall list for suppliers, staff, tenants, customers, and contractors.
- *Local resources*—Prepare a listing of local resources that may be needed during recovery operations, including local sources of labor, materials, equipment, and energy sources not identified elsewhere in the plan. Include the organization, points of contact, and the type of resource available.

4.3 Know What Functional Agreements Exist

This section provides information on site-specific emergency support agreements and mutual aid agreements required for preparing Tables 3-4 and 3-5 in Appendix A.

Document in the energy preparedness and operations plan what emergency support agreements exist between the site and utility service providers. Relative to each critical load, list the applicable utility companies, emergency support contracts, and emergency support contingency clauses. The list should indicate any support agreements that would apply if energy to a critical facility or load were lost.

Similarly, document in the plan any mutual aid agreements that exist between the site and state and local officials and organizations such as the Red Cross to assist in recovery efforts. List the organization, points of contact, and type of aid or service. Because these types of agreements are sometimes prepared and then mostly forgotten, this documentation may prove quite valuable. Any existing agreement should be located and then recalled and verified for each update of the energy security plan.

If mutual aid agreements do not exist or if certain necessary ones are found to have been overlooked, prepare remedial action items to correct the omissions.

4.4 Inventory and Manage Emergency Generators

This section pertains to emergency generator inventory and management information required to prepare Table 3-6 in Appendix A. The management of emergency generators is a critical part of energy security. Their reliability can be improved significantly if they are well maintained and tested on a regular schedule. Administrative controls should be used to ensure that generators are not taken for granted, a risk that tends to become higher at locations that benefit from highly reliable primary sources of electricity.

Inventory emergency generators, both fixed and portable, recording the following information:

- Generator ID and location
- Size (kW)
- Fuel source

- Operator
- Fuel storage capacity
- Fuel type
- Controls (auto or manual startup)

In addition, supply the following information:

- Plan for maintaining and testing fixed generators including maintenance of fuel supply
- Method for employing and maintaining portable generators
- Emergency fueling plan
- Designation and training of generator operators

4.5 Describe the Training Plan

This section provides information on the site's training plan that is needed to prepare Sect. 3.8 of Appendix A. Site management personnel should be trained annually on the details of the energy security plan and the specific procedures they should follow during energy outages. Therefore, prepare a plan and include it in the energy preparedness and operations plan that describes how site staff will be informed of training requirements and trained to respond effectively to energy emergencies.

Indicate in the training plan how staff will be made aware of their roles and responsibilities for interacting with local authorities, utilities, emergency responders, etc., and what the channels for communication will be during an emergency.

If training resources are not presently available at smaller sites, at least include the training requirements in the remedial action plan.

4.6 Review Energy-Related Construction Projects

This section provides information helpful in the review of project lists described in Sect. 3.9 in Appendix A. It is recommended that near the completion of the energy security plan analysis process site construction and operating and maintenance (O&M) projects be reviewed by the energy security manager, the energy security planning board, and/or energy security analysts to identify opportunities to introduce features that increase energy security.

The aim is not to perform a duplicate task identifying remedial actions, but to look for synergistic opportunities or cost-saving opportunities based on the planned construction work. For example, if there is a plan for installing an additional diesel storage tank, the location of the tank and its protection may need to be modified on the basis of the energy security analysis.

5. PREPARING A REMEDIAL ACTION PLAN

The energy security plan relies on the remedial action plan to specify proposed corrective actions. The corrective actions may be procedural, administrative, training, or physical upgrades to facilities and/or the energy infrastructure that serves the site. The remedial action plan states what is needed to improve energy security. Whether necessary actions are actually implemented depends on other factors such as obtaining new funding (see Sect. 5.4), especially when physical upgrades are proposed.

Energy infrastructure hardening can be accomplished through remedial actions based on the following approaches [11]:

- Access control
- Facility design
- Relocation
- Redundant sites
- System redundancy
  - —Multiple feeds
  - —Multiple fuels
  - —Multiple modes
  - —Mobility

5.1 Identify Remedial Actions for Unacceptable Risks

Identification of unacceptable risks is discussed in Sect. 3.5. Use the risks identified through this process as a basis for proposing remedial actions. List the proposed remedial actions or projects as briefly stated solutions resulting from a brainstorming process. Typically, list one to three solutions for each unacceptable risk. As seen in Appendix A, Table 2-5, the proposed ideas for remediation amount to only one column of a table. This is not a thorough, fully defined, and finalized listing of actions or projects for which funding should be sought.

Make the list of unacceptable risks and suggested steps for remediation brief so that the most urgently needed actions and projects do not become lost in the listing. Also, you gain little in identifying far more projects than will ever be funded. The most clearly justifiable remediation projects are those designed to address scenarios with a combination of high probability and high impact duration. Conversely, it would be difficult to justify not including at least one project to address such a scenario.

The first few years of the security assessment process are likely to result in remedial actions

designed to provide additional data to support future assessments. Examples may include keeping better records of energy outages and the time required for restoration, improving records of fires and accidents, preparing one-line diagrams of electrical distribution systems, and defining more precisely the records of site projects that may have energy security significance.

Although unacceptable risk is the primary basis for selecting remedial actions, consider the following best practices:

- *Listen to experts at the installation* — Outside analysts and contractors can make the mistake of taking an overly narrow view in proposing corrective actions based purely on an analytical perspective. The remedial action brainstorming process should be flexible and consider those projects strongly recommended by experts at the site. Site experts have the advantages of (1) understanding the idiosyncrasies of the energy systems and infrastructure, (2) knowing how the site works, (3) experiencing and reacting to energy outages, (4) knowing the dynamics and tendencies of emergency response organizations, and (5) knowing how to best meet mission goals under all contingencies (see Figure 8).
- *Consider quality technological solutions* — Projects recommended in part because they would be excellent technology demonstrations also may have significant merit. Such solutions may have the advantages of (1) addressing energy security in a broader scope, thus reducing unacceptable risks at several locations at a site; (2) saving energy costs, thus providing a project payback; and (3) providing more funding opportunities. One relatively extensive technological solution may replace many smaller-scale solutions and do so in a more effective or synergistic manner.
- *Conduct independent building surveys* — Surveys performed apart from the energy security assessment, such as an energy survey for a hospital, may identify projects that should be included in the remedial actions list.
- *Select high-priority actions* — If the list of proposed solutions becomes lengthy, employ some means to highlight what are considered to be the most urgently needed actions.

Figure 9 takes the energy security plan flow diagram (Figure 1) and adds to it many of the tasks described in this section. The figure shows how new remedial actions come not only from the listing of unacceptable risks, but also from the sources discussed above. The last additional source shown, "Projects from Prior Years," is discussed in Sect. 5.2. The analysts should also be aware of recent publications regarding approaches for mitigating risks to facilities. Examples of such publications currently being released are provided in the shaded box at the end of this section.

Figure 8. Site experts may introduce insightful projects such as a photovoltaic system to power critical circuits in a communications center. (Photo courtesy of Cooperative Community Energy)

In addition to the unacceptable risk and remediation table described here and in Sect. 3.5, a substantial amount of text may accompany the table to detail solutions and technology. If an energy consultant is acting as an analyst for the site, he will typically provide details about remedial actions and multiple technical alternatives at this stage in the process. An overzealous consultant may carry this to an extreme and overwhelm the energy security manager and planning board with too many overlapping technological solutions. Therefore, the manager and the board should ensure that the consultant clearly scopes each project and provides some form of guidance or a basis for making intelligent choices. Similar guidance should be provided in choosing between multiple small projects or one large project purported to have equivalent benefits for energy security. If a project will produce an energy savings or other type of cost savings, highlight this information, as it will be useful in obtaining funding.

Energy security may be perceived as a less tangible priority than other needs at a site, especially when management is focused on a monetary payback period. This brings up the issue of justifying projects on the basis of unique criteria and finding the necessary funding (see Sect. 5.4).

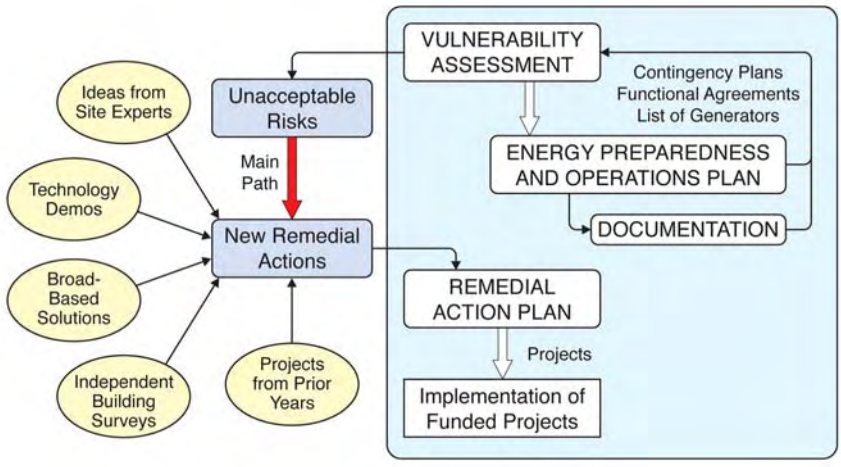

Figure 9. Energy security program flow diagram (see Figure 1) modified to show the transition from the vulnerability assessment to remedial action.

A How-To Guide to Mitigating the Risk of Potential Terrorist Attacks Against Buildings

The following information is based on a presentation by Milagros Kennett, Project Officer for the Risk Management Series, Mitigation Division, EP&R, FEMA/Department of Homeland Security, seminar on Tools and Techniques for Threat Assessment/Mitigation, Washington, DC, November 4, 2004.

FEMA is preparing and issuing a series of unclassified documents that will be of interest to building managers, schools, and the government. These documents, described on the FEMA web site, discuss ways to provide protection from physical threats (natural and intentional) to buildings (in pre- and post-construction phases) and the appropriate responses to threats. Examples are FEMA 426, 427, 428, 429, and 452, and the E155 course. Future issues are FEMA 430, 453, 455, and 459. Natural disasters are covered in FEMA 395 through FEMA 399.

FEMA 452, "How to Mitigate Potential Terrorist Attacks," is intended to facilitate risk assessment for man-made hazards and its integration into building design and/or building rehabilitation. It provides helpful information on (1) identifying and quantifying the value of assets, (2) evaluating the potential vulnerability of the critical assets to a broad range of identified threats, and (3) determining mitigation measures. To support the risk assessment process, an easy-to-use Risk Assessment Database is provided. This database is a stand-alone application that has functions to import and display digital photos, emergency plans, digital floor plans, and certain GIS products. The risk assessment core is composed of 42 pages of questions regarding the building(s). The software prioritizes major vulnerabilities among a large number of buildings and identifies and ranks mitigation efforts.

5.2 Address Project Lists from Prior Years

In parallel with identifying new proposed remedial actions, planners should review energy security projects from prior years that were never funded. If it is determined, based on the most recent energy security assessment, that certain of those projects should be carried over into the present listing of remedial actions, carefully merge them into the table to supplement the new remedial actions.

The energy security projects from prior years that are funded should also be reviewed to determine if completing those tasks would eliminate any of the unacceptable risks identified in the most recent assessment. In other words, make sure that no funded project was overlooked.

Finally, review the list of funded projects from prior years to make sure that each one is still valid and optimal based on (1) the most recent list of unacceptable risks, (2) the present or predicted status of energy systems at the site, and (3) potential solutions based on newly available technology.

5.3 Prepare a Remedial Action Plan

This section provides information that will help in preparing remedial actions that must be listed in Table 4-1 in Appendix A. Remedial actions are required for each unacceptable risk identified during the vulnerability assessment process.

The remedial action plan consists primarily of a table containing columns denoting (1) existing deficiencies, (2) corrective actions, (3) budgeted costs, and (4) status of each item.

The table contains primarily *budgeted* projects for improving energy security. Hence, table cells may be empty or nonexistent in the first year of an energy security assessment unless pre-assessment energy security projects existed, or unless certain high-priority projects are entered in the first two columns, leaving the "budgeting" and "status" columns empty. In subsequent years, update and expand the table as needed.

The importance of this table cannot be overemphasized. It designates the energy security solutions. It is recommended that the energy security manager maintain a working copy of the table throughout the year to be used in budgeting efforts and to track overall progress. This practice will ensure that the manager does not lose sight of key goals and milestones. When the time comes to document the table in the remedial action plan, the table will serve as a readily available snapshot of the status of funded projects at that time.

5.4 Identify Alternatives for Funding Remediation Projects

Identifying and obtaining funding for energy security projects is an ongoing process that may be comparable in difficulty to the energy security assessment itself. This section discusses alternatives for obtaining funding for proposed energy security projects of all types.

Depending on trends, budget crises, and the current emphasis on national security in the federal government, resources may range from available to mostly unavailable. In any case, the energy security manager should be aware of all funding alternatives and take the appropriate steps to request funding for energy security projects.

5.4.1 Funding based on project size

Small projects that involve purchases of items such as a propane heater or a small to medium-sized electrical generator can generally be funded using routine methods such as O&M funds. Small projects related to protection of assets, such as a fence or barricade around fuel storage, can likewise resort to routine funding such as for general site security or "force protection" in the case of the U.S. Army. Because of the relative ease of using routine resource channels, it is generally best not to cluster so many smaller projects together as to create a need for alternative funding. There can be other advantages to gradually phasing in general upgrades at a site, such as relying on a smaller contractor who may offer a more attractive quote if the work can be accomplished in installments or sequentially.

Small energy security projects funded from routine budget sources can be justified on the basis of security alone and do not have to have an inherent cost savings or a payback period. In the case of a large energy security project, more funding alternatives are available if there *is* an energy savings aspect. Fortunately, many or most large energy security projects can be designed to provide both an alternative/redundant source of energy and a cost savings over time. Common examples are distributed generation (DG) and co-generation (cogen)—or combined heat and power (CHP), as it is frequently called. In fact, the best DG/CHP economics are for large systems at energy-intensive sites (hospitals, military installations). Depending on the site location and local energy costs, the savings may be through (1) lower power generation costs, (2) peak shaving, (3) the use of waste heat, (4) special tariffs or utility incentive programs for conservation, and/or (5) reducing the emissions of harmful gases.

In locating funding for large energy security projects, best practices involve exploring a few potential sources of financing. Depending on the project, innovation, rather than a "best" or standard practice, can be a necessity. This will become quite apparent in the discussions that follow.

DG/CHP projects and similar-sized projects may be funded through the following means:

- Appropriated funds (e.g., MILCON)
- Third-party financing for the energy efficiency component
  - — Energy Savings Performance Contracts (ESPCs)
  - — Utility Energy Service Contracts (UESCs)
  - — Enhanced-Use Leasing (EUL)
- In connection with privatization contracts

5.4.2 Specific financing options

Planning, designing, and installing effective DG/CHP systems are complex and costly undertakings. At facilities that have strong technical and economic potential for CHP, the most common hurdles are limited staff time and funding to develop and build projects. Several financing options exist to help facility managers address these hurdles. The primary sources of funding that should be considered for large construction projects include the following. (See Ref. 11 for additional details.)

Appropriations/Military Construction (MILCON). Paying for an energy security project can involve federal and/or private resources. Federal appropriations have commonly been used for capital improvements such as emergency backup generator sets and for some small CHP systems. Special appropriations have subsidized demonstration DG/CHP projects employing small turbines (30–60 kW) and fuel cells (5–200 kW) at many installations. Appropriations are likely to continue to fund small projects and new technology demonstrations. But given utility privatization policies and budget priorities, the approval of significant numbers of large DG/CHP systems with MILCON funding is unlikely. Nearly all of the recent large CHP projects in the federal sector have been privately financed, and future projects will most likely continue to rely upon private funds.

Energy Savings Performance Contracts. ESPCs use an energy services company (ESCO) to develop and finance projects and guarantee a specified level of annual cost savings from the project. The ESCO provides all surveys, studies, designs, labor, materials, and equipment and is repaid from the guaranteed savings over the contract term. Contract terms are typically 10 to 20 years (the maximum is 25), after which the savings accrue to the agency. ESPCs require measurement, verification, and guarantees in a highly structured delivery order. Their standardized structure and pay-from-savings approach enable effective implementation of typical energy conservation measures (e.g., lighting; controls; heating, ventilation, and air-conditioning) without waiting for appropriations. However, an ESPC is intended to make improvements to government-owned facilities, and it sometimes creates hurdles for complex, unique projects like CHP that might more appropriately be privately built, owned, and operated. Examples of recent ESPCs for CHP at DoD sites include the Portsmouth Naval Shipyard (10 MW), the Southwest Division Naval Amphibious Base (120 kW), and the Marine Corps Base at Twenty-Nine Palms (7 MW), where energy security was a driving factor in the decision to proceed.

Utility Energy Services Contracts. UESCs are similar to ESPCs but are contracts with the serving utility for energy services and equipment. Special authorities permit streamlined, established-source selection, and flexibility in contracts. Guarantees and measurement and verification of savings are optional in UESCs, and some utilities prefer not to be involved in other follow-up services such as O&M and repair and replacement. Contract terms are generally limited to 10 years, making it more difficult to finance projects with long-term benefits (often the case with CHP). The viability of this approach also depends on the relationship with, and services offered by, the utility; some utilities are not interested in pursuing UESCs to develop DG/CHP projects.

5.4.3 Public-private energy ventures

The options that follow describe how DoD could lease property to a private developer who would then build, own, and operate the energy production plant and sell the commodities (electricity, steam, or chilled water) to the military and/or other customers.

Public-private energy ventures offer an alternative to government ownership and can permit energy services to be sold to third parties, thus spreading project risk. This authority was used successfully by the Navy to privately develop a geothermal energy project at China Lake, California. In the 1980s and 1990s, a few CHP energy projects were pursued using DoD's public-private venture authorities. The CHP projects were developed as procurements governed by the Federal Acquisition Regulation (FAR) and were generally structured so that the government was locked into a long-term, take-or-pay contract for energy services. In two cases of subsequent base realignment, the government had to pay a significant cancellation settlement, or continue paying for a greater amount of energy (steam) than required. Those experiences, coupled with the significant time and administrative costs required for a special, nonstandard procurement process compliant with FAR, and more recent mandates for utility privatization, apparently quelled interest in developing new CHP systems using the public-private venture authorities.

Enhanced-Use Lease (EUL). At the James H. Quillen Medical Center in Johnson City, Tennessee, the Veterans' Administration (VA) recently demonstrated how an agency can privately finance a large DG/CHP project (6.7 MW) while avoiding the risk of paying large cancellation costs. This was accomplished by structuring the transaction around their out-leasing authority, or EUL. Using EUL, a developer was selected and

given full responsibility for designing, financing, permitting, owning, and operating the CHP systems on VA property transferred under a long-term (35-year) lease. Under the EUL business plan, the VA agreed to purchase energy commodities (electricity, steam, and chilled water) from the new plant under favorable terms (compared with those available from the existing utility providers), based on a two-year contract with automatic renewal provisions. The developer was also authorized to sell energy commodities to third parties. It took a little over two years to complete the transaction and reach an arrangement that balanced the federal desire to limit risk with the private-sector need for sufficient guarantees to permit financing. See "The Leasing Alternative" in the boxed text for additional details.

Utility privatization. DoD facilities are actively implementing a policy to privatize ownership of energy distribution assets (poles and wires, pipes, etc.) on military bases unless continued government ownership is required for security purposes or unless privatization would be uneconomical. The privatization guidance requires transfer of ownership and allows the bases to sign long-term contracts for related energy services as the distribution assets are sold. Federal regulations must be followed to ensure open competition and receipt of a fair price for assets. Though the commodity may be included, very few utility privatization contracts include the electricity commodity. The contracts have not generally included an incentive to improve energy security and efficiency or to expand on-site generation capacity. However, in the interest of energy security, such incentives should be incorporated in the terms of the privatization contract whenever possible to meet energy security remedial actions. DoD installation managers responsible for addressing energy security could benefit from being informed about all available financing authorities, including utility privatization, in order to choose the approach that is most advantageous in meeting their needs.

The Leasing Alternative

The Veterans' Administration (VA) recently used an EUL to finance a 6.7-MW DG/CHP installation.

The final agreements in the VA contract provided adequate security to the developer by including automatic contract renewal provisions, an exemption from any "termination for convenience" clause, long-term energy sales to a third party, and the security of the long-term lease, as well as on VA strategic plans, site investments, and other factors verified through due diligence by the financier.

The energy service agreement avoided federal liability to pay remaining costs of the CHP system should specific conditions (closure or significant reduction in hospital occupancy) dictate that the VA not renew the energy services agreement prior to full term for financing. The Office of Management and Budget approved the two-year energy service agreement as an "operating lease" without the need to score the capital costs of the project. The energy services are financed from the VA's annual appropriations for operations and maintenance.

The military's longstanding leasing authorities were recently enhanced to facilitate projects similar to the VA's, but these have not yet been applied to any large DG/CHP project.

While the expanded military authority is flexible, few energy managers are aware of how it could be used to finance a DG/CHP project; and like the VA's, it requires project approval at the Secretary's level.

Both authorities allow long-term out-lease contracts, up to 75 years for the VA and longer for DoD, if they are found to be in the best interest of the military, with the lease term determined on a case-by-case basis. The basic steps in the DoD lease process are to (1) identify the potential project, (2) prepare the property for approval to lease, (3) market the property (notice of intent to lease), (4) select a developer, (5) develop a business management and leasing plan, and (6) sign and manage the lease.

The Army has prepared a special web site with a guide to out-leasing Army assets, with forms and spreadsheets to facilitate the process for installation managers.

The table below summarizes the relevant characteristics of the various authorities that could permit a federal site to finance and install a large energy-related construction project. "Maximum term" refers to the limit in years that an agreement could be effective under a given authority. The sixth column indicates who would pay the remaining cost of the project in the event of termination for convenience (e.g., if unforeseen base realignment or closure means the project is no longer needed by the government). Assignment of risk can vary depending on specific contract terms and is often shared to some degree. The table reflects who carries most of the risk in the CHP projects studied to date using different authorities [12]. "Agile option" refers to whether or not procurement is based on indefinite-delivery, indefinite-quantity (IDIQ), or established source. Of course, exceptions to most rules are possible.

All of the private financing approaches could allow the federal sponsors to tap private-sector project development expertise as well as overcome the lack of direct funding. Site-specific characteristics may make one option more appealing than another. Of the various forms of financing, ESPCs and UESCs have been used much more than other authorities for large energy conservation projects, primarily because of the ease of procurement and focused marketing and support of services by contractors (and special agency teams). In the case of ESPCs and UESCs, the Federal Energy Management Program (FEMP) and federal user agencies working with private partners have invested significant resources to streamline, standardize, and continually improve the processes, and experienced teams devoted to the use of these authorities are in place.

Options for financing federal DG/CHP projects: comparison of typical project characteristics

Financing authority	Legal basis	Source of funds	Max. term (years)	Asset owner	Risk if TFC[a] occurs	Agile option	Approval level
Appropriations	Congressional budget line item	Federal	NA	Govt.	Govt.	Varies	Congress, military appropriations legislation
ESPC	10 USC 2865 42 USC 8287	Private funds	25	Govt.	Govt.	Yes	Agency contracting officer; notice to Congress if >$10M
UESC	42 USC 8256 10 USC 2865	Private funds	10	Govt.	Govt.	Yes	Agency contracting officer
Public/private ventures	10 USC 2394 10 USC 2867	Private funds	30	Private owner	Terms define	No	Congress if >$10M; Secretary of Defense
EUL	38 USC 8161	Private funds	75	Private owner	NA – Private	No	Secretary of VA after 60-day notice to Congress
Enhanced lease (DoD) as proposed	10 USC 2667	Private funds	In-definite	Private owner	Private owner	No	Secretary of military dept. after 45-day notice to Congress
Utility privatization	10 USC 2688	Private funds	50	Private owner	Terms define	No	Secretary of military dept. after 21-day notice to Congress

[a]TFC = termination for convenience.

5.4.4 Streamlining and managing projects

Ease of procurement is an important factor in determining the development of DG/CHP. To reduce costly lead times, the government has employed umbrella, or IDIQ, contracts for specialized goods and services. Agencies can take advantage of IDIQ contracts to obtain services from various providers selected on the basis of their specialized capabilities. Since IDIQs are pre-competed, using these contracts saves agencies the time of developing and administering a formal request-for-proposals, bidding, and selection process. The necessary legal opinions, rules, and regulations to implement a new authority can be put in place prior to the IDIQ.

Under appropriations, each step of procurement—award, administration, and payment—must be managed in compliance with FAR. Under ESPCs and UESCs, the delivery order award and administration during both the implementation and performance phases are also structured to meet FAR requirements for construction and services in federally owned facilities. Under other alternative mechanisms, after a developer is selected, project contracting and financing is handled privately and can often follow more flexible and agile commercial practices. This can also save time and money. The enhanced-use lease approach is based on federal real property laws and regulations rather than FAR. Developer selection must still be documented for an out-leased DG/CHP project, and the energy commodity purchase is a separate agreement (in compliance with FAR) based on the lease business plan, but most project development tasks in between can be done on a commercial basis.

Most of the large federal CHP projects developed over the past decade have been financed under IDIQ ESPC and UESC authorities, with streamlined (pre-competed or established-source), standardized contracts and delivery order structures. Some DoD sites are interested in a more "privatized" approach to enhancing energy security with DG/CHP. The authorities for public-private ventures and leasing could address these issues, but they do not have a similarly streamlined and structured option available.

5.4.5 FEMP project assistance

FEMP provides technical and design assistance to help agencies resolve technical obstacles to project implementation. Technical assistance includes screening for project opportunities, performing feasibility studies, reviewing procurement specifications (including those for architect and engineer services), reviewing designs, and evaluating completed projects.

Federal agencies request assistance through a "Call for Projects" announced by FEMP every other year, or on an ad hoc basis through FEMP representatives in the regional offices. This approach allows federal agencies to identify their specific needs for assistance, and in turn allows FEMP to select the projects with the highest value. FEMP issues a Call for Projects in the following areas:

- sustainable new building design
- energy and water efficiency retrofits
- distributed generation and combined heat and power contributing to energy security and reliability
- renewable energy
- operations and maintenance

FEMP uses a competitive ranking process to select those projects that demonstrate the greatest value in terms of potential energy savings, replication, public education, and other benefits. Agencies are encouraged to share the cost of assistance.

6. PRACTICAL CONSIDERATIONS

This section discusses practical considerations for conducting an energy security assessment. The topics covered are the use of technical consultants, remaining cognizant of the site's mission, how the size of an installation can dramatically affect the process, the periodic update process, and the critical importance of information security relative to the energy security plan.

6.1 Decide Whether to Use Consultants

Except perhaps in the case of the smallest of sites or sites with few critical facilities, the energy security assessment process can generally benefit from the use of consultants. The general need for consultants is especially true during the first few assessments. However, if a small to medium-sized site already has a capable expert with experience in threat analysis and/or probabilistic vulnerability assessments, and the expert has adequate time available, there may be little advantage in bringing in a consultant. Whether to use an outside consultant may still depend on other factors such as how "energy-secure" the site is. If there is much work to be done in improving energy security and many unresolved issues, the assistance and insight of a consultant from the energy field is advisable.

A larger site can always benefit from the use of a consultant. In this case, it may be advantageous that the selection of a consultant be more restrictive. If the large site needs large or comprehensive solutions for energy security, a consultant should be selected from a company or

corporation that is capable of conceptualizing, defining, and clearly communicating such solutions. In this way, the installation can be presented with various options that will adequately address the technical challenges while being multifaceted in scope—addressing energy security, physical security, and energy conservation and cost savings.

Of course, there will be instances during certain years when a site needs a consultant but lacks resources to bring one in. Should this occur during the first year that an energy security assessment is performed at a site, the energy security manager and planning board (if one is used) would have to adhere to best practices and templates (such as the one provided in Appendix A) without going beyond reasonable limits. Rather than basing analyses and/or decisions on insufficient data or expertise, the site might have to list some steps in the process as remedial actions. Rather than recommend overly limited construction projects to fix a problem temporarily when better, longer-term solutions are needed, it might be best to defer some actions to later years. In the face of personnel shortages, perform a technically sound job on as many tasks as possible even if that means that others may have to be more fully addressed during the next iteration or funding year.

6.2 Tailor the Product to Your Site's Mission

The product that is needed for each site depends on its mission(s) or overall purpose and function and how critical each of its facilities is in meeting the mission(s). It may be justifiable for some sites to pursue a goal of becoming more robust, self-contained entities—attaining energy independence using a difficult-to-interrupt energy infrastructure. Other missions may dictate that the site become more fully integrated into the surrounding community with an energy system that can benefit both site and off-site needs depending on circumstances or situations that might arise.

Mission-critical facilities may have one or more of the following missions, among others:

- Deployment of forces
- Strategic defense site operations
- Personnel training
- Logistical support/resupply operations
- Protecting national assets
- Homeland security
- Chemical/biological studies
- Rapid response
- Community protection
- Community service
- Command center
- Communication
- Public health

Conduct the energy security assessment in such a way that the analysts do not lose sight of the need to balance mission-related, community-interactive, and off-site energy needs. The energy security manager should ensure that analysts keep a balanced approach consistent with meeting the needs of the mission.

6.3 Adjust the Approach to the Size of Your Installation

The energy security needs of a smaller site are often readily apparent if the energy security assessment is well executed by capable analysts. The remedial actions are generally straightforward and of limited scope, including items such as improved record keeping, better barriers around assets, a new building generator, and installation of an additional fuel storage tank.

As discussed in Sects. 5.4 and 6.1, larger sites may require large, multifaceted, and/or comprehensive solutions to meet their energy security needs and successfully secure funding. This may require making use of state-of-the-art technologies or technologies that may require some development or adaptation before being implemented at the site. The assessment of unacceptable risks and determination of remedial actions require considerably more evaluation at large sites to ensure that the final list of projects represents a good balance between smaller projects and broad-scoped projects. This means that the projects do not overlap each other in correcting unacceptable risks, the projects are cost-effective, funding is attainable, the need will remain until they are completed, and on-site energy savings will be accomplished when possible. Projects that increase combustion emissions should be avoided. Projects that provide energy redundancy and/or dual fuel capability are desirable, especially when they provide a payback.

Energy production and/or distribution at large sites is difficult to manage, especially during an energy outage or energy emergency. Even if plant personnel are well trained and good procedures are in place, the absence of information on what is occurring at any given time in any portion of the site can severely hamper the response effort. Therefore, large sites can often justify the costs of comprehensive information and control systems and intelligent control systems that are designed to facilitate a rapid response. Many of these systems include, or interface with, supervisory control and data acquisition systems and facility management systems.

6.4 Maintain Ongoing Reviews and Updates

The execution of energy security assessments is an iterative process. This approach is used to ensure that (1) changes that occur at a site are factored into the assessment; (2) energy security remains a high priority at each site; and (3) all documentation, remedial actions, and funding efforts are kept current and active. Depending on the site, the energy security assessments may proceed rapidly to completion or the process may prove cumbersome or ponderous (generally at large and complex sites). In all cases, schedule and pace the process so that all major blocks are completed during the year. At worst, this may mean that the greater part of certain subtasks or elemental tasks is deferred to the following year. The goal should be to document as much reference information as possible in the energy preparedness and operations plan and to complete a list of remedial actions. Refinements can come in subsequent years.

This approach ensures that a single energy security assessment does not become a multiyear process. Scheduling and completing all stages of the process during the first year sets a precedent at the site and helps to ensure that updates in following years will likewise be completed. Ideally, there will be an intervening period of several months each year when the energy security manager will be able to spend much of his or her time pursuing the funding and implementation of energy security projects.

6.5 Assure Information Security

The energy security plan outlines the vulnerabilities of a site's energy infrastructure and energy "feeds" from off-site sources. Thus, a great deal of sensitive information is compiled in one place. In addition, certain threat scenarios discuss how energy systems can be intentionally forced off-line. Obviously, take care to ensure that the very document that is intended to be used as a tool for improving energy security is not misused to accomplish the opposite.

The energy security plan should be classified as a For Official Use Only (FOUO) document, and an appendix containing all information describing the site's (1) single-point-of-failure vulnerabilities and (2) list of remedial actions should be classified as confidential. Extensive listings of remedial actions for a site are sensitive, since they clearly imply what the site's most serious vulnerabilities are. Using this approach, much of the energy security plan, including the vulnerability analysis, is documented in the appendix to the plan. The energy preparedness and operations plan, which is intended to be a readily available reference during energy outages, is appropriately designated FOUO. Actual energy-related project listings, generally a small subset of the remedial actions, would be either FOUO or unclassified so that funding and contracting efforts are not impeded.

7. REFERENCES

1. *Guide for Using Template for Energy Security Plans in Compliance With DEPPM 92-1*, FEMP, Washington, D.C., expected issue date: 2005.
2. G. Padgett, "Patterns of Atlantic Intense Hurricane Activity," Feature of the Month for June, http://www.weathermatrix.net/archive/tropical/summaries-2002/0005.html, July 2002.
3. R. Davidson, H. Liu, et al., "Hurricane Vulnerability of Electric Power Distribution Systems in the Carolinas," http://cee.ce.uiuc.edu/research/usnzworkshop/davidson.pdf.
4. National Earthquake Information Center (NEIC), http://neic.usgs.gov/.
5. Dr. C. Wood, *Volcano World*, University of North Dakota, http://volcano.und.nodak.edu, 1995.
6. N.C. Division of Emergency Management, Hazard Mitigation Section, http://www.dem.dcc.state.nc .us --- Ice storms in North Carolina.
7. K. Jones, models prepared by CRREL based on NOAA storm data, 1959–present, http://www.americanlifelinesalliance.org/pdf/iceload.pdf, ice storm table at http://www.americanlifelinesalliance.org/pdf/IceStormSummaries.pdf.
8. State Climate Office of North Carolina, North Carolina State University, http://www.nc-climate.ncsu.edu/climate/winter/background.html.
9. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations," IEEE Std 500-1984, Nuclear Power Engineering Committee of the IEEE Power Engineering Society, 1983.
10. "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems," IEEE Std 493-1997, Power Systems Reliability Subcommittee of the Power Systems Engineering Committee, IEEE Industry Applications Society, December 1997.

APPENDIX A:

ENERGY SECURITY PLAN TEMPLATE

The energy security plan template provided in this appendix is structurally complete with a sample cover page prepared for the U.S. Army, a table of contents, a list of tables, blank tables, etc. Text that is highlighted in yellow provides specific instructions, and the highlighted text should be deleted as the document is completed. Additional text is generally added to each section, as needed, to adequately introduce/describe tables and to provide required plans, test programs, training program details, etc. All elements and template text should be reviewed and revised as appropriate.

This template represents the basic requirements of DEPPM 92-1 for the U.S. Army. Installations of other federal agencies may be required to develop plans with substantial changes to accommodate site-specific circumstances and requirements. In such cases, the template will likely serve as only a starting point.

As described in Sect. 6.5, “Assure Information Security,” it is recommended that, in the interest of information security, the document be split up into a portion for official use only and a confidential annex. Sections 2 and 4 of the template would be included in the confidential annex. The final determination of how the information will be protected is ultimately made by each federal agency preparing an energy security plan.

ENERGY SECURITY PLAN IN COMPLIANCE WITH DEPPM 92-1

Vulnerability Assessment
Energy Preparedness and Operations Plan
Remedial Action Plan

[Installation Name]
[Date]

IMPORTANT: To use this template, see the *Guide for Using Template for Energy Security Plans in Compliance with DEPPM 92-1*. Information in the guide is essential for completing energy security plans in compliance with DEPPM 92-1.

Approvals

This Energy Security Plan addresses emergency planning requirements specific to [name of installation] energy system(s). This plan addresses the electric system, natural gas system, [propane/fuel oil], and steam/hot water].

This plan satisfies the requirement to develop and maintain a preparedness plan contained in DoD Policy 92-1, "Department Of Defense Energy Security Policy," dated 14 January 1992.

Prepared by:

[Plan writer's name] [plan writer's organization]	Date

Approved by:

[Garrison commander's name, rank] garrison commander [installation name]	Date

Contents

[Note: For many installations, the information security officer will require Sects. 2.5, 2.6, 4, and Appendix A to be broken out into a separate CONFIDENTIAL annex report with the main report designated FOUO. Be sure to address all information security issues and obtain security reviews of the document(s) as required.]

List of Tables

Energy Security Plans in Compliance with DEPPM 92-1

1. INTRODUCTION

1.1 Purpose and Scope

This plan addresses the policy stated in DEPPM 92-1: "It is a basic responsibility of Defense managers and commanders to know the vulnerability of their missions and facilities to energy disruptions and the risk of such disruptions, whether the energy source is internal or external to the command. Lastly, it is essential to take action to eliminate critical energy support vulnerabilities."

This plan for [installation name] includes the electric system, natural gas system, [propane/fuel oil/coal], and steam/hot water].

The purpose of this plan is to identify necessary actions, efforts, and resources required to restore energy systems to critical facilities and functions in accordance with DoD Policy Memorandum 92-1, dated January 14, 1992, "Department of Defense Energy Security Policy."

The Energy Security Plan includes an energy vulnerability analysis (section 2), an energy emergency preparedness and operations plan (section 3), and a remedial action plan (section 4). Mobility fuel is not included in this plan.

1.2 Plan Review and Revision Requirements

The Public Works Business Center (PWBC) is responsible for at least one annual review of this plan and ongoing maintenance to update key contacts and other information when necessary. The PWBC will monitor progress toward the milestones in the remedial action plan and report status to the [installation Commander on a quarterly] basis until actions are complete.

1.3 Coordination with Existing Policies and Procedures

This plan will be compatible and coordinated with existing force protection, security, emergency response, and other applicable policies and procedures.

1.4 Energy Security Planning Board [optional]

Table 1-1 lists the members of the energy security planning board who participated in a series of meetings designed to move the energy security plan preparation efforts forward through completion.

Table 1-1 Energy Security Planning Board

Position/Title	Name	Duty phone	Cell/other phone

2. ENERGY VULNERABILITY ANALYSIS

A vulnerability analysis was carried out to identify and characterize the vulnerabilities of [Installation]'s missions and facilities to energy disruptions and the risk of such disruptions. (The complete analysis is attached as Appendix A.) Key results of the analysis are displayed in this section.

The unacceptable risks identified by the analysis (given in Table 2-6) are the basis for the remedial action plan in section 4.

Defense managers and commanders will review energy vulnerability analyses annually to ensure that they are current.

2.1 Critical Facilities and Energy Requirements

Table 2-1 lists critical facilities and functions, and their energy requirements for meeting critical loads. This data will help in allocating funding and manpower resources, both for planning of remedial actions and for recovery during an emergency.

Notes below the table describe the data in each column.

Table 2-1 Critical Facilities and Energy Requirements

Priority[1]	Facility[2]	Critical function[3]	Critical energy requirement[4]

[1]The priority given to each critical facility as identified by tenants and customers.
[2]Building number (or other identifier) of each critical facility. List specific panel, meter, and location within the facility if it can be managed as a distinct critical load.
[3]Type of function or critical use/mission: (a) life/health and public safety, (b) communications, (c) core support for critical missions, (d) environmental systems, or (e) other special emergency functions.
[4]Indicate the quantified minimum amount of energy required to meet critical loads in an emergency (e.g., KW for electricity, Btu/hr for steam).

2.2 Critical On-Site Energy Sources and Emergency Responsibilities

Table 2-2 shows the priority critical loads from Table 2-1 and identifies utility energy sources and energy supply/storage infrastructure within the installation that support the critical loads. These energy sources are essential to the facility and will be evaluated relative to their reliability, vulnerability, and/or history of causing incidents at the installation. The table also lists the rating or capacity of the primary energy sources.

In column 5, the table lists what backup energy sources are available, including the total capacity of dedicated emergency backup generators and, if applicable, portable generators (indicate "portable"). (Details on generators are inventoried in Appendix [_].)

In the last column, the table identifies the parties responsible for operation, maintenance, repair, or replacement of these critical energy sources in an emergency, including staff, suppliers, customers, and tenants.

Notes below the table describe the data in each column.

Table 2-2 Critical On-Site Energy Sources and Emergency Responsibilities

Priority [1]	Facility[2]	Energy sources[3]	Rating/Capacity of source[4]	Backup energy source[5]	Responsible party, contact information[6]
Electrical System					
Natural gas system					
Steam system					
Fuel oil					
Portable generators					

[1, 2]From Table 2-1.
[3]Utilities/energy source (e.g., electricity, natural gas, steam heat, chilled water, etc.) critical to maintaining the critical function.
[4]Rating/capacity of the energy source.
[5]The first-response, emergency backup equipment or plan and who is responsible for it. Specify the type of startup or control system used (e.g., manually start vs. auto start, need for human intervention or an essential transfer switch).
[6]Party responsible for operation, scheduled maintenance, testing, and repair/replacement. Also, contact information for determining operating capacity and limitations during an emergency.

2.3 Critical Off-Site Energy Systems and Emergency Responsibilities

Table 2-3 lists the energy systems (e.g., main feeders) outside the installation that support critical loads (from Table 2-1) as well as utility service providers' responsibilities to repair or replace them in emergencies.

Note that emergency support agreements with utility service providers are addressed in section 3.4.

Table 2-3 Critical Off-Site Energy Systems and Emergency Responsibilities

Priority [1]	Facility[2]	Critical system[3]	Rating / Capacity[4]	Responsible party, contact information[5]	Plans to repair or replace in emergency[6]
Electrical system					

Natural gas system					
Steam system					
Fuel oil					

[1, 2]From Table 2-1.
[3]Selected energy systems, such as main feeders, supporting the critical loads listed in Table 2-1. The systems may serve one or more critical facilities, the whole installation or sub-installation.
[4]Rating/capacity (e.g. electrical cable size/voltage) of the feeder.
[5]Party responsible for operation, scheduled maintenance, testing, and repair/replacement. Also, contact information for determining operating capacity and limitations during an emergency.
[6]Plans for repairing or replacing critical system in case of failure.

2.4 Portable Energy Generator Needs

This section identifies those critical facilities that are known (by analysis or experience) to have an especially strong potential need for portable power generators. For each of these portable generator needs, the power generation capacity, physical location and method of transportation is indicated.

Information pertaining to the full listing of portable (and dedicated) generators is provided in section 3.6. [Provide listing here or indicate "No heightened short-term potential needs for specific portable generator applications are known to exist."]

2.5 Risks of Disruption of Energy Supplies

Table 2-4 lists the potential initiators or event scenarios that may cause energy disruptions at [installation name]. The table includes the estimated probability of the initiating event occurring, the estimated duration of impact on energy systems and supplies, what amount of warning (if any) may be expected in terms of days, and the person responsible for monitoring the vulnerability. A probabilistic vulnerability analysis, documented in Appendix A, provides the basis for the data recorded in the table.

Table 2-4 Threats to Critical Energy Supplies

Initiating Event	Estimated probability of initiator	Estimated duration of impact on energy system (average/maximum)[1]				Warning expected	Person monitoring risk
		Electric	Natural gas	Propane / fuel oil	Steam / hot water		
Objective Risks							
Earthquake							
Flood							
Hurricane							
Tornado							
Tidal wave							
Extreme heat							
Fire							
Accidents							
Mechanical or electronic system failures							
Subjective Risks							
Labor strike / contract default							
Sabotage / terrorism/ riots							
Arson /vandalism							
Cyber attacks on computer/ control systems							
Other Significant Potential Disruptions							

[1]Lists the expected (or average) duration of impact and the maximum duration of impact on energy services based on the scenario. Indicates the estimated disruption in days or weeks.

2.6 Unacceptable Risks

An unacceptable risk has a combination of high probability and severe consequence (e.g. long duration) that cannot be tolerated at the installation. Table 2-5 shows the unacceptable risks that were identified using the results of the vulnerability analysis. The remedial action plan to address prioritized unacceptable risks is in Section 4. See Appendix A for the complete energy vulnerability analysis.

Table 2-5 Unacceptable Risks

Priority [1]	Facility [2]	Threat/scenario	Impact	Recommended remediation
Electrical system				
Natural gas system				
Steam system				
Fuel oil				
Portable generators				

[1, 2] From Table 2-1.

3. ENERGY EMERGENCY PREPAREDNESS AND OPERATIONS PLAN

3.1 Alternate Modes of Maintaining Critical Functions

Table 3-1 outlines procedures for executing critical base missions in the absence of normal energy supplies and certain secondary energy supplies. "Secondary energy supplies" may include items such as dedicated generations at a critical facility. Identifying alternate means of continuing the mission is a highly creative and often difficult planning exercise that is well worth the effort. Energy emergency response teams should be trained to make use of this information when energy disruptions and additional supply difficulties coincide.

Table 3-1 Alternate modes of maintaining critical functions

Priority [1]	Facility[2]	Critical function[3]	Alternate mode of maintaining critical function

[1, 2]From Table 2-1.
[3]From Table 2-1: Type of function or critical use/mission: (a) life/health and public safety, (b) communications, (c) core support for critical missions, (d) environmental systems, or (e) other special emergency functions.

3.2 Communications and Emergency Personnel Contact Information

Key authorities to contact in an energy emergency are listed in Table 3-2. The table includes personnel from the installation, DoD, other federal, state and local emergency officials, intelligence officials, and others who would need to be contacted.

Table 3-2 Emergency personnel contact information

Title	Individual	Duty/Home/Cell Telephone
Installation		
Installation Commander		
Garrison Commander		
Executive Officer (XO)		
Installation Coordinator(s)		
Director of Public Works*		
DPW, O&M Division Chief		
DPW, Housing Division Chief		
DPW, EMO Chief		
Provost Marshall		
Fire Marshall		
Public Affairs Officer		

Title	Individual	Duty/Home/Cell Telephone
Commissary Officer		
COE Representative		
Other DoD		
Other federal		
Intelligence officials		
State and local emergency		
[Contractor representatives]		
[Utility representatives]		
[Preventive medicine}		
[Major tenants]		
[Other]		

3.2.1 Assignment of Radio Frequencies for Emergency Communications

Radio frequencies for communication during emergency response and recovery efforts are assigned as follows:

[Alternatively, reference applicable document]

3.3 Personnel Recall Procedures

Table 3-3 outlines personnel recall procedures for energy emergencies. Suppliers, other staff, tenants, customers, and contractors who would be needed are identified, with their emergency work assignments and contact information.

Table 3-3 Personnel Recall Procedures

Title	Name	Telephone numbers	Emergency work assignments
		Duty: Home: Cell:	
		Duty:	

Title	Name	Telephone numbers	Emergency work assignments
		Home: Cell:	
		Duty: Home: Cell:	
		Duty: Home: Cell:	
		Duty: Home: Cell:	
		Duty: Home: Cell:	
		Duty: Home: Cell:	
		Duty: Home: Cell:	

3.4 Emergency Support Agreements with Utility Service Providers

Table 3-4 lists the critical energy requirements that were identified for utility service providers to ensure that critical mission areas are recognized in the service restoration plans of those providers. Emergency support contingency clauses contained in the utility service contracts for restoring service for those critical loads are summarized in the table.

Current utility service contracts are [indicate documents and/or location, or include documents as Appendix __].

Table 3-4 Emergency Support Agreements with Utility Service Providers

Critical load identified	Utility company and contact	Emergency support contingency clauses for restoring critical loads
	[Utility company] [Name] [Position/Title] [Telephone No.]	

3.5 Mutual Aid Agreements

Installations are required to negotiate mutual aid agreements, as necessary, with state and local officials to assist in installation recovery efforts, in community recovery efforts, and to minimize loss of life in outlying communities.

Mutual aid agreements have been established with several organizations. These organizations, contact information, and a description of the types of aid and services available via the agreements are listed in Table 3-5. Complete

copies of these agreements are available [indicate documents and/or location, or include documents in Appendix __].

Table 3-5 Mutual Aid Agreements

Organization	Points of contact	Types of aid or services available
	[Name] [Position/Title] [Duty Telephone No. / Emergency No.]	[Describe types of aid/services available through the existing mutual aid agreement, e.g., personnel, materials, security, etc.]

3.6 Inventory of Generators

[Table 3-6 or Appendix [__]] is an inventory of emergency generators, installed, portable, and contracted/on call. The table indicates the generator identification number and type, the power rating, the type of fuel required, the fuel tank size, the designated operator, and essential control information needed for operation. This information is maintained by [name] and will be kept current.

Table 3-6 Inventory of Generators

Generator ID and location (F=fixed or dedicated, P=portable)	Power rating (kW)	Fuel type	Fuel capacity (gal)	Operator	Special controls or manual switching required

Method for Employing and Maintaining Portable Generators

[Describe required plan here.]

Emergency Fueling Plan

[Describe required plan here.]

Designation and Training of Generator Operators

[Describe required plan here.]

Maintenance and Testing of Generators

[Describe required plan here.]

3.7 Other Local Resources for Use in Recovery Operations

The local sources of labor, materials, equipment, and energy identified (other than public utilities and mutual aid agreements) are listed in Table 3-7.

Table 3-7 Other resources for use in recovery operations

Organization	Points of contact	Types of resources available
	[Name] [Position/Title] [Duty phone No. / Emergency No.]	[Describe other resources available locally (labor, materials, equipment, energy) for use in recovery operations]

3.8 Training

[Describe training plan here.]

3.9 Review of Construction Projects

Installations' energy security plans are required to facilitate review of construction projects for (1) adequate energy security planning and (2) for consideration of the impact that the projects will have on the existing recovery plan.

[Describe review of construction projects here.]

4. REMEDIAL ACTION PLAN

The remedial action plan identifies corrective actions required to mitigate unacceptable risks that may result in energy disruptions. Table 4-1 lists the existing deficiency or unacceptable risk, the corrective action that the installation plans to implement, the budgeting for the action, and the current status.

The status of the remedial action plan will be reviewed at least annually.

Table 4-1 Remedial Action Plan

Existing Deficiency	Corrective Action	Budgeting	Status

5. REFERENCES

[References cited in the Energy Security Plan.]

APPENDIX A: COMPLETE ENERGY VULNERABILITY ANALYSIS

[Append energy vulnerability analysis to the Energy Security Plan.]

A Strong Energy Portfolio for a Strong America

Energy efficiency and clean, renewable energy will mean a stronger economy, cleaner environment, and greater energy independence for America. Working with a wide array of state, community, industry, and university partners, the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy invests in a diverse portfolio of energy technologies.

Produced for the U.S. Department of Energy, Energy Efficiency and Renewable Energy, Federal Energy Management Program, by Oak Ridge National Laboratory.
1/06

For more information contact:
EERE Information Center
1-877-EERE-INF (1-877-337-3463)

www.eere.energy.gov/femp

U.S. Department of Energy
Energy Efficiency and Renewable Energy

Bringing you a prosperous future where energy is clean, abundant, reliable, and affordable.