Preamble:
It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the bulk electric system. Guidelines provide suggested guidance on a particular topic for use by bulk electric system entities according to each entity’s facts and circumstances and not to provide binding norms, establish mandatory reliability standards, or be used to monitor or enforce compliance.

Introduction:
This Guideline addresses potential risks that can apply to some Electricity Sector Organizations and provides practices that can help mitigate the risks. Each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.

As the foundation of any company’s security program, physical security practices and measures help ensure the safety and security of a company’s personnel, assets, and information. By providing the basic concepts of physical security and common practices and measures available to electric sector organizations, the guideline should enable companies to develop a physical security plan that matches the level of accepted risk for each of their facilities.

Each entity should implement physical security measures at their facilities to safeguard personnel and prevent unauthorized access to assets, business processes, control systems, equipment, and sensitive information that may be resident in the facility. Each entity should implement physical security solutions in a way that is consistent with the criticality of the business processes and assets in that facility and sufficient to provide appropriate situational awareness of activity so that the entity can initiate an appropriate and timely response.

Scope of Application:
This guideline applies to facilities and functions that support the reliability of the electricity infrastructure, as well as the business processes and the overall operation of the individual organization. Each entity, using a risk assessment methodology, should define and identify those facilities and functions it believes to be critical to operations, key assets or otherwise prioritized and deemed important (i.e. a tiered approach specific to each company’s operations). Keeping in mind that the ability to mitigate the loss of a facility or function through redundancies may make some facilities less critical than others.

This Risk Assessment Methodology (RAM) should be a consistent and standard methodology to ensure important factors are not overlooked.
Per the NERC definition, a “critical” facility may be defined as any facility or combination of facilities, that, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Attended facilities like control centers, communication facilities, and corporate offices, present a different physical security challenge because they tend to be more complex, centralized, and have multiple physical perimeters. While the more centralized nature of attended facilities allows more economy of scale, this advantage is balanced against the risks associated with common points of failure and cascade effects associated with a single event. NERC cyber security standards specifically address many of the physical security needs of attended facilities in the following sections:

- Physical Security Perimeter[s]
- Physical Access Controls
- Personnel
- Monitoring Physical Access
- Systems Management
- Physical Incident Response Actions

In addition, attended, critical facilities typically require many more support assets such as UPS, chilled water, redundant external power supply, environmental controls, and communication infrastructure that the typical unattended facility would not require. Since these support assets are fundamental to the reliable operation of the critical facility, they are themselves critical assets and require appropriate physical protection.

Identification of critical/key/prioritized physical assets can be accomplished by using criteria based on national security, public health and safety, economic security, regional and national electric grid reliability, and integration of generation into the grid. Facilities to consider include:

- Substations/Switchyards
- Generating Plants
- Control Centers/Administrative Sites
- Transmission Infrastructure

**General Guidelines:**

The NERC document “An Approach to Action for the Electricity Sector” version 1.0 dated June 2001, identifies a four-tiered approach to physical security. An effective program usually encompasses all four of these components:
Avoidance: Ensure electric power system integrity and availability by promoting the development and implementation of security policies, standards, and procedures; by use of outreach programs; and by providing education programs to enhance and maintain appropriate levels of cyber and physical cyber security.

Assurance: Ensure electric power system integrity and availability by promoting the regular evaluation of physical and cyber security measures. A sub-tier component includes the identification of appropriate levels of risk management.

Detection: Protect electric power systems through monitoring, identification, central reporting and analysis of operational, physical and cyber threats and/or incidents. Promote reporting of threat warnings and threat prevention information back to ES operating regions and utilities.

Recovery: promote methods for timely investigation of operational, physical or cyber security incidents and rapid recovery/restoration of services supporting the delivery of electric power services. Lessons Learned from this layer are incorporated into the other tiers.

Physical Security Concepts Overview

Together, these concepts, if applied, provide a consistent “systems approach” to designing and implementing physical security measures that will mitigate the impact on assets should a physical attack occur.

Physical security typically comprises eight distinct concepts, these are:

- **Deter** – visible physical security measures installed to induce individuals to seek other less secure targets.
- **Detect** – physical security measures installed to detect unauthorized intrusion and provide local and/or remote intruder annunciation.
- **Delay** – physical security measures installed to delay an intruder’s access to a physical asset and provide time for incident assessment and response.
- **Assess** – the process of evaluating the legitimacy of an alarm and the procedural steps required to respond.
- **Communicate** – communication systems utilized to send and receive alarm/video signals and voice and data information. Also, includes the documented process to communicate detected intrusions.
- **Respond** – the immediate measures taken to assess, interrupt, and/or apprehend an intruder.
- **Intelligence** – measures designed to collect, process, analyze, evaluate and interpret information on potential threats.
- **Audit** – the review and inspection of physical security measures to evaluate effectiveness.

Each entity should prioritize its sites and associated supporting assets. This prioritization should consider risks based on factors such as prior history of incidents, threat warnings from law
enforcement agencies, loss of load consequences, response time, recovery time, and overall operating requirements. Each entity also should consider an inspection and assessment program to review existing security systems and to make recommendations for appropriate changes. (See guideline for conducting vulnerability assessments.)

**Guideline Details:**
Determining the types of physical security measures and processes required can be complicated by the many options available. When designing, implementing, or auditing a physical security program, organizations should consider the following.

“Protection in Depth” and Crime Prevention Through Environmental Design (CPTED) concepts should be implemented and considered in the design phase of any physical security program.

**Protection in Depth defined (abbreviated)** – A strategy that seeks to delay rather than prevent the advance of an attacker, buying time by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over a period of time allowing time to respond.
Crime Prevention Through Environmental Design (CPTED) – Crime prevention through environmental design is an approach to problem solving that considers environmental conditions and the opportunities they offer for crime or other unintended and undesirable behaviors. CPTED attempts to reduce or eliminate those opportunities by using elements of the environment to (1) control access; (2) provide opportunities to see and be seen; and (3) define ownership and encourage the maintenance of territory.\(^1\)

The details included below can generally be implemented with currently available technology:

1. fencing, walls, gates, and other barriers to restrict access to the facility for both safety and security purposes;
2. limiting access to authorized persons through measures such as unique keying systems, “smart locks,” high-security locks, access card systems, or the use of security personnel;
3. access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e., photo ids, visitors passes, contractor ids) to be displayed while in the site/facility;
4. alarm systems to monitor entry into site/facility grounds;
5. perimeter alarm systems to monitor forced intrusion into and surveillance of the site/facility;
6. alarms, CCTV, and other security systems reporting to an attended central security station that can then be evaluated and entity personnel or law enforcement authorities dispatched to investigate a potential problem;
7. guards (special events or targeted);
8. vehicle barriers;
9. adequate lighting; that provides visibility for observation and optimum CCTV functionality;
10. signage; to warn potential intruders;
11. a comprehensive security awareness program;
12. roving security patrols or fixed station security staffing;
13. projectile barrier to project vulnerable equipment or personnel;
14. security surveys and other risk assessment programs; and
15. the levels of physical security measures may be increased or lowered based on changes in threat levels, evolving threat scenarios, and facility risk categories.

Physical security systems should be augmented in accordance with the “Threat Alert System and Physical Response Guidelines for the Electricity Sector” based on changes in threat levels, scenarios,\(^1\)

---

1 For a more detailed introduction to CPTED, see Crowe (2000), Crowe and Zahm (1994), and National Crime Prevention Council (1997)
and categories. In designing a physical security system, the objective of the intruder should be considered. The four major objectives in describing an intruder’s behavior are:

- Damaging, operating, or tampering with site/facility operational equipment and controls,
- Stealing or damaging site/facility operational equipment, materials, or information,
- Threatening the safety of entity personnel or customers,
- Creating adverse publicity and inducing fear.

To ensure the effectiveness of installed or procedural security measures, each organization should also consider an inspection and survey program to review existing security systems and procedures and make recommendations for appropriate changes as necessary.

1. Each entity should have a security policy or procedures in place to manage and control access into and out of the site. These policies should clearly state what practices are prohibited, which ones are allowed, and what is expected of all personnel with access to the site. The site security policies should clearly define roles, responsibilities, and procedures for access and should be part of an overall “critical” infrastructure protection policy.

2. The physical security perimeters at each site should be clearly identified. All physical access points through each perimeter should be identified and documented. Most sites typically have at least two physical security perimeters such as the fence and the building.

3. Physical access controls should be implemented at each identified perimeter access point. All access into and out of “critical” sites should be recorded and maintained for a period of time consistent with NERC standards. At minimum, these records should indicate the name of person(s) entering the site, their business purpose, their entity affiliation, time in, and time out.

4. Access into and out of “critical” sites should be monitored with authorization procedures. Site access may be authorized by the system or security operator if not performed by electronic means such as a card reader where authorization is predetermined. Security measures are not an alternative to security procedures; if the facility is both unmanned and energized, it is recommended that any personnel entering it contact the system or security operator and advise them that they are there, even if a card reader is in place.

5. Records that identify all entity, contractor, vendor and service personnel who have unescorted access privileges to sites should be identified and documented. While most entity personnel will have unescorted access to all sites; contractors and vendors should only have unescorted access to sites they have contractual business in.

6. All contractors and vendors with “critical” site access privileges should be required to pass a background screening before being issued an entity-provided contractor ID badge. Only those contractors with entity-issued ID badges should be granted unescorted site access. Contractors and vendors must be aware of the utility security practice. They must read and sign to acknowledge that they understand and will act according to those security measures. Even in these circumstances, an entity employee with unescorted access to the site should...
confirm and monitor the contractor’s activity while in the site appropriately.

7. A site incident response program should be established that at a minimum would provide a rapid assessment of events in the site in order to differentiate normal electromechanical failures from malicious acts. If malicious activity is evident, the priority should be to notify law enforcement, based on established arrangements/plans and return the site to normal functionality while preserving forensic evidence where possible.

8. Entities should avoid dual use of critical site grounds for non-critical functions where possible. They should eliminate or restrict the use of the site secure area for non-critical activities such as equipment storage, non-critical asset storage, contractor staging, and personal vehicle parking. If dual use is unavoidable, the entity should consider the establishment of another physical security perimeter that excludes the non-critical activities from the site secure area, or the entire area should conform to this security guideline.

Identification of critical/key/prioritized physical assets, can be accomplished by using criteria based on national security, public health and safety, economic security, regional and national electric grid reliability, and integration of generation into the grid. Facilities to consider include:

- **Substations/Switchyards**

  Substations/switchyards are common elements in the electric industry and are often unattended. Substations contain many of the fundamental assets necessary for the transmission and distribution of electric power to customers. Transformers, breakers, busses, switches, capacitor banks, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs), and communication systems can reside within the confines of the substation. The compromise of any one of these elements can impact the integrity of the electric grid, depending on the amount and type of load being served by this substation at the time of the incident.

  Many subs have a control building within them that is a roofed structure typically designed to protect electronic equipment and switch gear. While most substations will logically be located in or near major load centers, in urban, suburban, and industrial/commercial sites, others are located with interregional ties in remote/rural substations and may be just as important for interconnection purposes.

  The effectiveness of security methods differs greatly from site to site. In general, more rigorous security measures should be applied to the more important substations. Protection in depth/CPTED principles can be applied starting with the perimeter fence, landscaping, lighting, signage, etc. Special consideration should be given to wash outs under the fence, vegetation management, and standard maintenance protocols may include security inspections. Mobile security systems, routine/random security patrol and law enforcement liaison can also be
applied. Additional security enhancements to mitigate metal theft can be applied as well; for more information on these programs see link “Copper Theft Strategies”.

- **Generating Plants**

There are several types of generating plants (Fossil Fuel, Nuclear, Hydro, Combustion Turbine and Combined Cycle. Fossil fuel and nuclear plants typically involve huge operations consisting of numerous structures spread over several acres with large numbers of actual and potential entry points onto the site. Hydro plants tend to be contained within or adjacent to massive structures (dams), but have a lesser amount of unauthorized access potential. Combustion turbine and combined cycle plants typically have a smaller overall footprint; however, they consist of numerous separate structures spread over a more open environment. All generally have switchyards associated with them. These are controlled by a stand-alone switch-house/electronic control building, or their operations may be incorporated into the plant’s generation electronic control center. Regardless of their location, these control stations encompass the same critical cyber assets as do the substations annotated above. Although, generation plants are generally staffed 24/7; they cover a substantial amount of area and have a widely dispersed work force. Further, stand-alone switch-houses/electronic control buildings, which may or may not be located within the plant’s primary security perimeter, are not routinely attended, particularly at night and on weekends.

By their very nature, generation plants as well as the associated critical cyber assets controlling them are essential elements of the bulk electric system. Therefore, robust security measures must be taken to protect them to ensure the overall integrity and reliability of the grid. Things to consider would be to ensure the entire property perimeter is properly fenced. Pay special attention to water-based approaches as many plants reside on or very near large bodies of water or rivers. Zones/layers of protection may be applied starting with the perimeter fence, utilizing the buildings walls/openings, and protecting the inner-most sensitive areas such as control rooms, labs, etc. Physical security concepts should also be applied to areas that contain hazardous chemicals. In power plants, the Packaged Electronic/Electrical Control Compartment (an unmanned room that an operator can control the plant from) should be afforded the same degree of protection as the Control Center.

- **Control Centers/Administrative Offices**

Control Centers are particularly important because they offer an attacker a full range of options – from within its confines they can damage or destroy rotating equipment or SCADA systems, they can injure or kill operating personnel, they can access the interconnected grid to introduce malware, or they can hold the facility hostage by barricading themselves in and demanding
concessions. Protection priorities in Control Rooms are: first, deny entry to unauthorized personnel; and second, identify and log all entering personnel.

Administrative Offices should be protected as any office structure within your company would be giving due consideration to the risks inherent at its location. Consideration should be given to access control, identity management, and regulatory compliance. Administrative offices are generally not considered critical from the perspective of the BES, but they may be considered official by their company or entity.

- **Transmission Infrastructure**

  High-voltage transmission lines, and the associated support towers, form the backbone of the electric power grid. Much of this infrastructure is located in isolated areas. These “Transmission Line Corridors” (T-Line Corridors) can present significant risk and physical security challenges.

  Protection in depth/CPTED principles can be applied at the areas surrounding the base of the towers similar to any other physical asset. Additional consideration may be given to protecting areas where the lines come to a 90 degree angle, areas of interdependencies, areas where lines cross rails, rivers, etc. Coordination with standard operational inspections, including aerial, to ensure security issues are being addressed is one way to mitigate the risks.

**Definitions:**
The following definitions apply in this guideline.

**Access Control System** – A means of electronic access where the access rights of personnel are predefined in a computer database. Access rights may differ from one physical perimeter to another.

**Special Locks** – These may include locks with non-reproducible keys, magnetic locks that must be opened remotely, and possibly some sort of interlock system that restricts access through one perimeter while another is open. This includes the family of high-security locks, which have hardened components, pick proof keyways, shrouded shackles, and un-producible keys. Also need “key control” program.

**Security Guard (roving)** – Either staff or contract security personnel may randomly patrol multiple facilities. This asset is typically used for special events, periods of high threat levels, areas experiencing high intrusion levels, or that serve as a staging area for construction. Also known as a mobile patrol.

**Fence** – This is the minimal security asset and usually defines the first physical security perimeter encountered at the site/facility. There are several levels of fencing ranging from solid material, to standard chain link fencing (most common), to cable reinforced chain link fence.
Video Surveillance – Video Surveillance can be very effective in operational settings. Examples of pre-processed video surveillance that captures images of activity in the site/facility preceding a site/facility security alarm can provide the system operator a “quick review” of the site/facility alarm incident.

Door & Gate Open (SCADA) – These alarms are typically based on some sort of “contact status” that indicates a door or gate has been opened. These alarms are particularly useful when used in conjunction with some sort of “attended station” status. Note: While these alarms, if received via SCADA will, at most, represent only a handful of additional status points for the most critical substation, appropriate attention to RTU scan loading should be considered.

Alarm System – These systems typically incorporate several security solutions into a surveillance and alarm package. These package solutions are usually specific to a high-risk site/facility, do not interface with any other system, and are set up to provide enhanced forensic evidence at that site.

Intrusion Detectors – These devices use various means to detect intrusion in a specific area. These systems can sometimes generate false alerts in an open environment.

Entity – The facility or asset owner, operator, etc.

Critical Asset – Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Intruder – Any unauthorized individual or any individual performing unauthorized activity within the site/facility, regardless of whether or not they are physically present at the time of the unauthorized activity.

Physical Security Perimeter – A gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.

Security Assets – Fences, gates, alarm systems, guards, and other security elements that can individually or as a system be applied to a facility to maintain reliability or reduce risk.

Secure Area – The area contained within the first or outer physical security perimeter.

Protection in Depth – The strategy of forming layers of protection of an asset. A strategy that seeks to delay rather than prevent the advance of an attacker, buying time by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over a period of time allowing time to respond.

Crime Prevention Through Environmental Design (CPTED) - Crime prevention through environmental design is an approach to problem solving that considers environmental conditions and the opportunities they offer for crime or other unintended and undesirable behaviors. CPTED attempts to reduce or eliminate those opportunities by using elements of the environment to (1) control access; (2)
provide opportunities to see and be seen; and (3) define ownership and encourage the maintenance of territory. (See Footnote 1)

Related Documents and Links:
Security Guidelines for the Electricity Sector: Guideline Overview

- Physical Response
- Vulnerability and Threat Assessment
- Threat Response and Incident Reporting
- Emergency Plans
- Continuity of Business Processes
- Communications
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information


Internet links:

• Copper Theft

Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Version Number</th>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/14/2002</td>
<td>1.0</td>
<td>Initial Version</td>
</tr>
<tr>
<td>5/17/2004</td>
<td>0.01</td>
<td>Split out this draft into a separate guideline from the Physical Security Guideline and made several grammatical and content changes.</td>
</tr>
<tr>
<td>6/7/2004</td>
<td>0.02</td>
<td>Various wording changes. Added page numbers, alarm system description, and removed several Internet links.</td>
</tr>
<tr>
<td>7/20/2004</td>
<td>0.04</td>
<td>Various grammatical changes. Replace “must” with “should” where appropriate. Separated matrix example better. Introduced reference to Threat Alert System and Physical Response Guidelines for the Electricity Sector. Defined Intruder. Eliminated surveillance in Item 5 Under General Guidelines. Replaced “three years” with “consistent with NERC Standards”.</td>
</tr>
<tr>
<td>8/16/2004</td>
<td>0.05</td>
<td>Various wording and grammatical changes. Altered definitions of critical facility and critical asset to more closely match the definition in the NERC Overview Guideline. Changed all references to company to entity. Returned security elements to original order. Added “Where appropriate” to specific guidelines.</td>
</tr>
<tr>
<td>8/19/2004</td>
<td>0.06</td>
<td>Removed “bulk” from applicability. Removed construction from Specific Guideline 8.</td>
</tr>
<tr>
<td>9/16/2004</td>
<td>0.07</td>
<td>Various wording changes. Changed definition of</td>
</tr>
<tr>
<td>Date</td>
<td>Version</td>
<td>Changes</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10/15/2004</td>
<td>1.0</td>
<td>Approved by NERC Board of Trustees.</td>
</tr>
<tr>
<td>07/01/2007</td>
<td>1.5</td>
<td>Extensive updates and edits to make the text current and to incorporate the 2006 CIPC approved format for all guidelines.</td>
</tr>
<tr>
<td>07/22/11</td>
<td>1.81</td>
<td>Under Section “Specific Guidelines” created section for 4 general areas of focus.</td>
</tr>
<tr>
<td>08/17/11</td>
<td>1.82</td>
<td>Removed the “Security Asset Matrix”.</td>
</tr>
<tr>
<td>08/31/11</td>
<td>1.83</td>
<td>Reviewed, revised and/or removed the word “critical” throughout the document.</td>
</tr>
<tr>
<td>08/31/11</td>
<td>1.84</td>
<td>Inserted verbiage reference to “Protection in Depth” and “Crime Prevention Through Environmental Design”.</td>
</tr>
<tr>
<td>10/24/11</td>
<td>1.89</td>
<td>Formatted for CIPC 30-day review.</td>
</tr>
</tbody>
</table>