Security Guideline for the Electricity Sector: Physical Security

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 importance of the business processes and assets in that facility and sufficient to provide 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 essential to operations, key assets or otherwise deemed important and prioritized (i.e. a tiered approach specific to each company’s operations). Each entity should keep in mind that the ability to mitigate the loss of a facility or function through redundancies may make some facilities less essential than others.

This Risk Assessment Methodology (RAM) should be a consistent and standard methodology to ensure important factors are not overlooked. Common methodologies include NIST, RAMT, etc.
An essential asset/facility may be defined as any asset or facility or combination of assets and 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 boundaries. 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, essential facilities typically require many more support assets such as uninterruptable power supply, water, redundant external power supply, environmental controls, access controls, and communication infrastructure that the typical unattended facility would not require. Since these support assets are fundamental to the reliable operation of the essential facility, they are themselves essential assets and appropriate physical protection should be considered.

Identification of essential 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. An example of facilities to be considered:

- Substations/Switching Stations
- 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 electricity sector 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 the following eight distinct concepts. They are as follows:

• **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 to the site, recovery time, and overall operating requirements. Each entity also should consider an inspection and assessment program to review existing security processes and systems and to make recommendations for appropriate changes. (See Guideline for Conducting Vulnerability Assessments in the Related Documents and Links section.)

Guideline Details:
Determining the appropriate types of physical security measures and processes can be complicated by the many options available. When designing, implementing, or auditing a physical security program, organizations should consider “Protection in Depth” (PID) and Crime Prevention Through Environmental Design (CPTED). These concepts should be considered and implemented in the design phase of any physical security program.

Protection in Depth (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 suggested list of physical security measures below can generally be implemented with currently available products or technology:

- fencing, walls, gates, barriers, etc., to restrict access and limit visibility to the facility for both safety and security purposes;
- 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;
- access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e., photo identification, visitors passes, contractor ids) to be displayed while in the site/facility;
- alarm systems to monitor entry into site/facility grounds;
- perimeter alarm systems to monitor forced intrusion into and surveillance of the site/facility;
- alarms, closed circuit television (CCTV), and other security systems such as video surveillance management system with video analytics that detects intrusion 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;
- guards (special events or targeted );
- adequate lighting that provides visibility for observation and optimum CCTV functionality;
- signage to warn potential intruders;
- roving security patrols or fixed station security staffing;
- projectile barrier to protect vulnerable equipment or personnel; and
- security surveys and other risk assessment programs.
- a comprehensive security awareness program;

The levels of physical security measures may be increased or lowered based on evolving threat scenarios and facility risk categories. In designing a physical security plan, the objectives of the intruder should always be considered. The four major objectives in describing an intruder’s behavior are:

¹ For a more detailed introduction to CPTED, see Crowe (2000), Crowe and Zahm (1994), and National Crime Prevention Council (1997)

Security Guideline for the Electricity Sector: Physical Security

Approved by CIPC on June 20, 2012
• 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.

**Procedural Security Measures** - 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 infrastructure protection policy.

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

3. Physical access controls should be implemented at each identified access point. All access into and out of essential assets 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 entity affiliation, and time of entry. Other considerations could include exit time, escort name, business purpose, etc.

4. Access into and out of essential sites should be monitored with authorization procedures. The system or security operator may authorize site access if not performed by electronic means such as a card reader where authorization is predeterminated. 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 (and when they leave), even if a card reader is in place.

5. Documented records that identify all entity, contractor, vendor and service personnel who have unescorted access privileges to sites should be identified and maintained. While most entity personnel will have unescorted access to some or all sites, contractors and vendors should only have unescorted access to the sites for which they have contractual business.

6. Background screening should be considered for all contractors and vendors before being issued an entity-provided contractor identification badge. Only those contractors with entity-issued identification badges should be granted unescorted site access. Contractors and vendors should be made aware of the utility security practice. They should read and sign to acknowledge that they understand and will act according to those security measures. Periodic assessment of the contractor’s adherence to the security measures should be considered.

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 operational failures from malicious acts. If malicious activity is evident, the priority should be to notify law enforcement based on established arrangements or plans, and returning the site to normal functionality while preserving forensic evidence where possible.

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

9. Electricity sector entities should consider monitoring and sharing relevant intelligence and their analysis of sensitive threat and incident information between sector participants, the federal, state and provincial governments and amongst other critical infrastructures. Entities should consider participating in unclassified and classified briefings available through a number of sources including; Electricity Sector Information Sharing and Analysis Center (ESISAC), Infragard, Natural Resources Canada, Department of Homeland Security, Homeland Security Information Network (HSIN), federal, regional Fusion Centers, state, provincial and local law enforcement agencies.

**Identification of essential 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/Switching Stations**

  A “substation” (including switchyards at generating facilities) is an area of equipment containing switches, circuit breakers, buses, and transformers for switching power circuits and to transform power from one voltage to another or from one system to another.

  A “switching station” is a station where transmission lines are connected without power transformers.

  Substations and switching stations are common elements in the power system necessary for the transmission and distribution of electric power and are often unattended. Most stations have a control building within the perimeter fence containing batteries, relays, and control and communication equipment utilized for operation and protection of the power system (See Figure 1). The control building may also contain low-voltage or medium-voltage switchgear for
station service or supplying local loads. Typical control building designs provide a basic level of physical security and environmental protection.

Typical criteria for implementing substation physical security are based on an assessment of probability, frequency, duration and cost of occurrences, safety hazards, severity of damage, equipment type, number and type of customers served, substation location, design type, and criticality of load. For detailed guidance on physical security of substations and switching stations reference IEEE 1402, Guide for Electric Power Substation Physical and Electronic Security.

Additional security enhancements to mitigate metal theft can be applied as well; for more information on these programs see link “Copper Theft Strategies” in the Related Documents and Links section of this guideline.

- **Generating Plants**

There are several types of generating plants (e.g. Fossil Fuel, Nuclear, Hydro, Combustion Turbine and Combined Cycle.) Fossil fuel and nuclear plants typically involve extensive 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 (substations) associated with them. These are controlled by a stand-alone switch-house or control building, or their operations may be incorporated into the plant’s generation control center. Regardless of their location, these control stations encompass the same essential 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 or control buildings, which may or may not be located within the plant’s primary security boundary, are not routinely attended, particularly at night and on weekends.

By their very nature, generation plants as well as the associated cyber assets controlling them may be essential elements. Therefore, security measures should 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, See Fig. 1. 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 from which an operator can control the plant) 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, an attacker can damage or destroy rotating equipment or SCADA systems, they can cause dire harm to 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 and control centers 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 by giving due consideration to the inherent risks and the assets at its location. Consideration should be given to access control, identity management, and regulatory compliance.

- **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 to transmission lines and at the areas surrounding the base of the towers similar to any other physical asset. Redundant transmission lines and secure replacement materials should be considered as best practice. Additional consideration may be given to protecting areas where the lines come to a 90 degree angle, areas of intersection with other Critical Infrastructure/Key Resources (CIKR) 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.

---

2 Note that in the United States the Chemical Facility Anti-Terrorism Standard (CFATS) may be applicable to certain sites, and physical security measures should be implemented accordingly.
Definitions:
The following definitions apply in this guideline.

Alarm System – These systems typically incorporate several security solutions into a surveillance and alarm package.

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)

Critical Infrastructure / Key Resources (CI/KR)- Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction. Key Resources, as defined in the Homeland Security Act, are publicly or privately controlled resources essential to the minimal operations of the economy and government. 3

Entity – The facility or asset owner, operator.

Fence – A barrier that usually defines the first physical security boundary 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.

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.

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

Locks – These may include locks with non-reproducible keys, magnetic locks that are opened remotely, and possibly some sort of interlock system that restricts access through one boundary while another is open. This includes the family of high-security locks, which have hardened components, pick proof keyways, shrouded shackles, and un-reproducible keys that are part of a key control program.

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

Protection in Depth – The strategy of forming layers of protection of an asset. It is a strategy that seeks to delay rather than prevent the advance of an attacker, buying time by yielding space. Rather than

---

1 Note, reference the National Infrastructure Protection Plan (NIPP).
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.

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

**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.

**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. This is also known as a mobile patrol.

**Video Surveillance** – The use of cameras to transmit a signal to a specific place for monitoring.

**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:
• NERC CIP Standards CIP 001, http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

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. Replaced “must” with “should” where appropriate. Separated matrix and made example better. Introduced reference to Threat Alert System and Physical Response Guidelines for the Electricity Sector. Defined Intruder. Eliminated surveillance in Item 5</td>
</tr>
<tr>
<td>Date</td>
<td>Version</td>
<td>Changes</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8/16/2004</td>
<td>0.05</td>
<td>Under General Guidelines. Replaced “three years” with “consistent with NERC Standards”.</td>
</tr>
<tr>
<td>8/19/2004</td>
<td>0.06</td>
<td>Various wording and grammatical changes. Added “Where appropriate” to specific guidelines.</td>
</tr>
<tr>
<td>9/16/2004</td>
<td>0.07</td>
<td>Various wording changes. Changed definition of “Critical Asset” to that approved by CIPC. Added adjective “critical” as appropriate for clarification.</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>
<tr>
<td>01/10/2012</td>
<td>1.9</td>
<td>Updated from CIPC 30-day review and formatted for Industry 45-day review.</td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td>Approved by CIPC.</td>
</tr>
</tbody>
</table>