

Security Guidelines for the Electricity Sector: Physical Response

NERC	Guideline
Guideline Title: Physical Response	Version: 3.0
Effective Date: November 1, 2005 Revision Date: 2007	Approved by Board of Trustees: November 1, 2005

Preamble:

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.

Introduction:

This Physical Response Security Guideline is to provide North American electricity sector organizations¹ with the actions they should consider when responding to the threat level alerts issued by the U.S. Department of Homeland Security² (DHS) or Public Safety and Emergency Preparedness Canada³ (PSEPC). Threat alert levels may be issued nationally or for a specific geographical area, such as a region, city, or group of cities. The alerts could also be issued for a specific industry or facility type, such as generating stations, substations, or hydroelectric facilities. The guideline is a framework for developing a response plan for an organization-specific physical threat.

Purpose:

This guideline provides actions that electricity sector organizations should consider when responding to threat level alerts from the Electricity Sector Information Sharing and Analysis Center (ESISAC), DHS for U.S. organizations, or PSEPC for Canadian organizations. The intent is to help define the scope of actions each organization may implement for its specific response plan, based on the nature of the threat and the organization's specific requirements. Each organization must conduct its own assessment of vulnerability and risk to identify critical facilities and functions, and categorize the vulnerabilities and risks associated with those facilities and functions. Such an assessment will help identify countermeasures to mitigate threats and allow asset owners to make rational decisions about the level of protection needed.

Goals:

This guideline and the subsequent industry actions have two goals:

- Provide examples of security measures that other electricity sector organizations should consider when responding to threat level alerts.
- Achieve uniformity in the response actions of the electricity sector to threat level alerts.

Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of each electricity sector organization.

Each electricity sector organization is expected to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility or function through redundancies may make some facilities or functions less critical than others.

Security Guidelines for the Electricity Sector: Physical Response

From an industry-wide perspective, a critical facility or function may be defined as any facility, function, or combination thereof 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 to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

Process:

The process for communicating changes in threat level alerts includes the following:

1. Information on threats will be reported by electricity sector organizations to the ESISAC, where it will be assessed and communicated to DHS and other appropriate government and law enforcement agencies, or other electricity sector organizations.
2. Changes in the threat level alerts issued by DHS or PSEPC will be assessed by the ESISAC, either independently or in cooperation with DHS, PSEPC, and industry experts, and communicated to the electricity sector organizations.
3. To obtain additional information, or to verify the threat alert level, contact ESISAC at 609-452-1422 or info@nerc.com.
4. Information on the current threat level alert status, or to review the guidelines developed for the electricity sector is available at <http://www.esisac.com/>.

Physical Response Guidelines for the Threat Alert Levels:

The following are examples of physical security measures to be considered for each threat alert level. These examples are not intended to be an exhaustive or all-inclusive list of possible security measures. Not all measures are applicable to all organizations. An organization may decide to reorder the sequence of some measures it deems appropriate to its environment and responsibilities. Most organizations may need to develop additional, specific security measures beyond the scope of those listed below.

ES-Physical-Green (Low)

Definition: Each electricity sector organization's alert level response plan will establish the base level actions to be taken for the initial ES-Physical-Green (Low) threat level. The Low threat alert level applies when no known threat of terrorist activity exists or only a general concern exists about criminal activity, such as vandalism.

Response: This level warrants only routine security procedures. Any security measures applied should be maintainable indefinitely and without adverse impact to operations. This level is equivalent to normal daily operations. Action items to consider at the Low threat level include the following:

1. Ensure that normal security operating standards and procedures are in place and operational.
2. Train security staff and key personnel on all aspects of the response plan, as well as specific pre-planned operating standards and procedures.

Security Guidelines for the Electricity Sector: Physical Response

3. All visitors should be approved before allowing them entry into a critical facility or access to a critical system.
4. Stop individuals not known or otherwise approved to determine identity and reason for presence and take appropriate action, such as issuing a badge or removing the individual from the property.
5. Conduct routine maintenance and inspection of electronic security equipment so that equipment is maintained in good working order at all times.
6. Periodically post or issue workforce awareness messages, and conduct tabletop exercises as appropriate.
7. Review and update all security, threat, and disaster-recovery plans at least once every year.
8. Report to security or facility management any unusual or suspicious activity observed by critical facility personnel or contractors.
9. Address security topics at employee meetings to increase security awareness.
10. Annually audit electronic or other access programs for critical facilities to ensure proper access authorization.
11. Ensure proper training of hazardous material, security, and emergency response personnel.
12. Identify critical facility long-term and short-term security measures as appropriate. Examples of security measures are:
 - Electronic security systems
 - Closing nonessential perimeter and internal portals
 - Physical barriers such as bollards or concrete barriers
 - Fencing
 - Lighting
 - Security surveys
 - Vulnerability assessments
 - Availability of security resources — contract and proprietary
 - Law enforcement liaison
 - Ensure availability of essential spare parts for critical facilities

Security Guidelines for the Electricity Sector: Physical Response

ES-Physical-Blue (Guarded)

Definition: The ES-Physical-Blue (Guarded) threat level applies when a general threat of terrorist or increased criminal activity with no specific threat directed against the electric industry exists.

Response: The recommended security measures are additional to those listed for the Low threat level. The Guarded threat level should be maintainable for an indefinite period of time with minimum impact on normal electricity sector organization operations. Action items to consider at the Guarded threat level include:

13. Communicate the heightened security level to all personnel and contract workers at the critical facilities. The communication should include a reminder to be alert for unusual or suspicious activities and to whom such activities should be reported. Security staff at other, noncritical facilities also should be made aware of the increased threat level.
14. Monitor all deliveries, particularly deliveries of combustible materials such as start-up fuel, diesel fuel, and gasoline.
15. Review operational plans and procedures to ensure they are up to date. They should include the following:
 - a. Security, threat, disaster recovery, and fail-over plans
 - b. Other operation plans as appropriate, e.g., transmission control procedures
 - c. Availability of additional security personnel
 - d. Availability of medical emergency personnel
 - e. Review of all data and voice communications channels to assure operability, user familiarity, and backups function as designed
 - f. Review of fuel source requirements
16. Provide local law enforcement agencies with any information that would support their ability to provide assistance if called upon.
17. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

ES-Physical-Yellow (Elevated)

Definition: The ES-Physical-Yellow (Elevated) threat level applies when a general threat of terrorist or criminal activity directed against the electric industry exists.

Response: The recommended security measures are additional to those listed for Low and Guarded threat levels. Such measures are anticipated to last for an indefinite period of time. Action items to consider at the Elevated threat level include:

Security Guidelines for the Electricity Sector: Physical Response

18. Increase the surveillance of critical locations.
19. Ensure all gates, security doors, and security monitors are in working order, and that visitor, contractor, and employee access controls are enforced.
20. Notify critical and on-call personnel of the elevated threat level.
21. Establish and assure ongoing internal and external communications and coordinate the organization's action plan with local, state/provincial, and federal law enforcement agencies as appropriate.
22. Review operational plans and procedures and ensure they adequately address the terrorist threat associated with the reason(s) for the elevated threat level.
23. Identify additional business- and site-specific measures as appropriate.
24. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

ES-Physical-Orange (High)

Definition: The ES-Physical-Orange (High) threat alert level applies when a credible threat of terrorist or criminal activity directed against the electric industry on an international, national, or regional basis exists.

Response: The recommended security measures are additional to those listed for Low, Guarded, and Elevated threat levels. Such measures are anticipated to last for a defined period of time. Action items to consider at the High threat level include:

25. Communicate the heightened security level to all personnel and contract workers on site. The communication should include a reminder to be alert for unusual or suspicious activities and to whom such activities should be reported.
26. Coordinate the security of critical facilities with neighboring organizations including other electricity sector organizations and large customers.
27. Use communications channels with local, state/provincial, and federal law enforcement agencies and other emergency management agencies responsible for responding to the critical facility to assess the nature of any threats to the facility or organization.
28. Review related emergency action plans based on current intelligence and consider activation of alternate backup operational control and office centers as appropriate.
29. Place all essential critical facility support personnel on alert and consider conducting tabletop exercises.

Security Guidelines for the Electricity Sector: Physical Response

30. Consider deployment of additional security personnel if there is sufficient information to suggest a heightened probability of attack on the facility or the surrounding area.
31. Consider restricting parking around critical facilities.
32. Where appropriate, ensure all gates and security doors are locked and actively monitored twenty-four hours a day, seven days a week, either electronically, or by random patrol procedures.
33. Verify the identity of delivery personnel and conduct a general inspection of deliveries, if feasible, (for example, verify that paperwork is in order and the external appearance of deliveries is consistent with the paperwork).
34. Enforce strict control of visitors and visitor vehicles entering critical facilities.
35. Consider postponing or canceling nonessential tours and visits.
36. When appropriate, contact suppliers and coordinate with combustible deliveries as necessary.
37. Perform a periodic inspection of site fuel storage and hazardous material facilities.
38. To the extent practical, coordinate critical facility security with adjacent facilities.
39. Consider making immediate repairs and return to service any essential equipment that is inoperable due to repair or maintenance. If possible, suspend scheduled maintenance for essential equipment.
40. Coordinate security related media releases with security, media relations, and management.
41. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

ES-Physical-Red (Severe)

Definition: The ES-Physical-Red (Severe) threat level applies when a terrorist or criminal act against any segment of the North American electric industry occurs or credible intelligence information indicates such an act is imminent or has occurred.

Response: This alert level may apply as a result of either an incident that occurs in North America outside of the electricity sector, or a threat from an international, national, or regional incident. During this period, maximum-security measures will be recommended and all security measures defined for Low to High threat levels shall be enacted as appropriate to each electricity sector organization. The duration of a Severe alert will be defined by the incident, but it is not intended to remain in place for a substantial period of time. Implementation of such measures

Security Guidelines for the Electricity Sector: Physical Response

could cause hardship on personnel and could seriously impact facility business and security activities. Actions items to be considered at the Severe threat level include:

42. Communicate the heightened security level to all on-site personnel. The communication should include a request to be alert for unusual or suspicious activities and to whom such activities should be reported. Ensure all on-site personnel are fully briefed on emergency procedures and emergency conditions as they develop.
43. Contact local, state/provincial, and federal law enforcement and other government agencies to determine the nature of the threat and its applicability to operations. Establish frequent communications with all appropriate law enforcement agencies for two-way updates on threat status.
44. Unless conditions dictate otherwise, open emergency center(s).
45. Account for all personnel at affected locations.
46. Unless circumstances dictate otherwise, deploy additional security resources to critical facilities.
47. Consider the release of nonessential personnel depending on the nature of the threat or incident.
48. Discontinue all tours and visitors.
49. Consider discontinuing mail and package deliveries to critical facilities.
50. Consider suspending maintenance work on essential equipment, except work that management determines to be emergency work and critical.
51. Continuously monitor or otherwise secure all entrances to critical service facilities. This step may include use of armed security personnel or off-duty law enforcement officers.
52. Inspect all vehicles entering every facility.
53. Identify and implement plans for any additional measures specific to the facility as appropriate based on available intelligence.
54. If feasible, close public access areas such as boat ramps and recreation areas. If these facilities are part of projects licensed by the Federal Energy Regulatory Commission (FERC), inform the FERC regional office of the decision as soon as practical.
55. Continue to monitor the situation and be prepared to de-escalate to a lower threat alert level.

Security Guidelines for the Electricity Sector: Physical Response

56. Monitor conditions and be prepared to de-escalate to a lower threat level.

Revision History:

Date	Version Number	Reason/Comments
June 14, 2002	1.0	Issuance of the ESISAC-developed four-state threat condition model (ThreatCon Normal, Low, Medium, and High). Document titled, <i>Threat Response</i> .
October 8, 2002	2.0	Update of physical guidelines to the five-state threat model released by DHS in August 2002. Updated document titled, <i>Threat Alert System and Physical Response Guidelines for the Electricity Sector</i> .
November 1, 2005	3.0	Update of the five-state threat model to incorporate additional action items and to reformat document to the guideline format approved by the Critical Infrastructure Protection Committee (CIPC). Updated document titled, <i>Security Guideline – Physical Response</i> .

¹ These threat alert levels and physical response guidelines do not apply to facilities regulated by the U.S. Nuclear Regulatory Commission.

² <http://www.dhs.gov/dhspublic/display?theme=29>. The DHS Homeland Security Advisory System is a color-coded threat level system used to communicate with public safety officials and the public at large so that protective measures can be implemented to reduce the likelihood or impact of an attack.

³ http://www.psepc.gc.ca/index_e.asp.