
Preamble:
This guideline addresses potential risks that can apply to some electricity sub-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 provides North American electricity sub-sector organizations with the actions they should consider when responding to the threat alerts issued by the U.S. Department of Homeland Security (DHS), Public Safety and Emergency Preparedness Canada (PSEPC). Threat alerts may be issued nationally or for a specific geographical area, such as a region, city, or group of cities. Threat alerts could also be issued for a specific industry or facility type, such as generating stations, substations, or hydroelectric facilities. This guideline is a suggested framework for developing a response plan for an organization-specific physical threat.

Purpose:
This guideline provides actions that electricity Sub-sector organizations should consider when responding to threat alerts from 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 should 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 guide organizations to rational decisions about the level of protection needed.

Goals:
This guideline and the subsequent industry actions have two goals:
- Support entities development of response actions to threat alerts.
- Support consistency to electric sector entities response action to threat alerts.
- Provide examples of security measures that other electricity Sub-sector organizations should consider when responding to threat 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 sub-sector organization. Each electricity sub-sector organization should self-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.

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 alerts includes the following:

1. Information on threats should be reported by electricity sub-sector organizations to the ES-ISAC, where it will be accessed and communicated to DHS and other appropriate government and law enforcement agencies, or other electricity sub-sector organizations.

2. Changes in the threat alerts issued by DHS or PSEPC will be assessed by the ES-ISAC, either independently or in cooperation with DHS, PSEPC, and industry experts, and communicated to the electricity sub-sector organizations.

3. To obtain additional information, or to verify the threat alert, contact ES-ISAC (24 x 7) at 404-446-9780 or esisac@nerc.com.

4. Information on the current threat alert status, or to review the guidelines developed for the electricity sub-sector is available at http://www.esisac.com.

5. Appendix “A” of this document has been developed for the possible use as a flip chart/checklist, produced in hard copy, and to be utilized at a local site.

**Physical Response Guidelines for the Threat Levels:**
The following are examples of physical security measures to be considered for each threat condition. 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 and should fall within legal parameters. An organization may decide to revise or reorder the sequence of some measures or threat levels it deems appropriate to its environment, responsibilities and within legal parameters. Most organizations may need to develop additional, specific security measures beyond the scope of those listed below.

<table>
<thead>
<tr>
<th>Normal Operations/Best Practices</th>
<th>1 – 18 Items for consideration:</th>
</tr>
</thead>
</table>

**Definition:** The Baseline 1-18 are actions recommended when no known threat of terrorist activity exists or only a general concern exists about criminal activity, such as vandalism. Each electricity sub-sector organization’s alert level response plan will establish the baseline actions to be in place.

**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 Baseline level 1 – 18 include the following:
1. Confirm normal security operating procedures are current, in place, and operational.

2. Provide training and updates for security staff and key personnel on all aspects of the response plan, as well as specific pre-planned operating procedures.

3. Periodically issue workforce security awareness messages.

4. Train mail handling personnel and all employees handling mail directly on-site on the characteristics of suspicious mail or packages. Review response procedures for these items.

5. Brief on timely and threat related security topics at employee meetings to increase security awareness.

6. Provide reoccurring training of hazardous material, security, and emergency response personnel.

7. No persons should be permitted access to the facility without proper authorization by authorized management.

8. Authorized persons will adhere to access control procedures and prevent tailgating or other unauthorized entry.

9. Identification badges, permanent or temporary are required for all individuals onsite, including employees, contractors, and visitors.

10. Individuals or persons not possessing or displaying an identification badge should be challenged to determine their identity and reason for their presence. Appropriate action should be taken upon this determination.

11. Visitors should receive visitors badges, be required to sign in, providing appropriate identification to verify their identity.

12. Annually audit electronic or other access programs for critical facilities to ensure proper access authorization.

13. Conduct routine maintenance and inspection of security equipment to ensure that it is in good working order.

14. Conduct routine security inspections and patrols of the facility and critical areas and components and reports submitted of findings.

15. Conduct periodic security tabletop exercises with facility and/or executive management as appropriate. Consider involvement of law enforcement support as well as tour of facilities for familiarity of response.

16. Review and update all security, threat, cyber, business continuity, and disaster-recovery plans on an ongoing basis or at least once every year.

17. Unusual or suspicious activities observed by personnel should be reported to local law enforcement, local management and security.
18. Identify critical facility long-term and short-term security measures as appropriate. Examples of security measures are:

- Electronic security systems (locks, alarms, cameras, access control, etc.)
- Closing nonessential perimeter and internal portals
- Identify and secure all essential perimeter and internal portals and establish accountability
- Physical barriers such as bollards or concrete barriers
- Perimeter signage
- Fence integrity
- Lighting effectiveness
- Security surveys
- Vulnerability assessments
- Availability of security resources – contract and proprietary
- Law enforcement liaison (FBI, jurisdictional law enforcement agencies, Fusion Center, etc)
- Maintain essential spare parts for critical facilities

<table>
<thead>
<tr>
<th>Elevated Risk</th>
<th>19-50 Items for consideration:</th>
</tr>
</thead>
</table>

**Definition:** The Elevated Risk 19-50 are actions recommended when a general or 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 the Baseline level 1. The Elevated Risk actions listed here should be maintainable for an indefinite period of time with minimum impact on normal electricity sub-sector organization operations. Action items to consider at the Elevated risk level include:

19. Communicate the heightened alert level to all security staff and onsite personnel at the critical facilities. This should include vendors with routine deliveries. The communication should include a reminder to be alert for unusual or suspicious activities and to where it should be reported. Security staff at other, noncritical facilities also should be made aware of the increased threat level.

20. Inform local law enforcement agencies that the facility is at an elevated alert level, confirm communications methods to be utilized and advise them of security measures being employed. Request that agencies increase the frequency of patrols at critical facilities.

21. Security personnel should review company security and incident response plans and procedures.

22. Review operational plans and procedures to ensure they adequately address the threat associated with the reason(s) for the elevated alert level. They should include the following:
   a. Security, threat, disaster recovery, fail-over plans, and business continuity 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
g. Review vehicle search procedures.

23. Limit facility access to required visitors, personnel, and vehicles.

24. Increase surveillance of critical areas and facilities.

25. Monitor and restrict all deliveries. Particularly deliveries of combustible materials such as startup fuel, diesel fuel, and gasoline. Confirm delivery with receiving personnel. Request list(s) of anticipated deliveries of those essential to continued operations.

26. 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)

27. Conduct random inspections of vehicles, bags, backpacks, purses, etc.

28. Ensure all gates, security doors, and security monitors are in working order, and that visitor, contractor, and employee access controls are enforced.

29. Evaluate the necessity of non-vital maintenance and capital project work that could affect facility security. Delay or reschedule this work as appropriate.

30. Increase lighting in facility buffer zones, if feasible.

31. 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.

32. Verify the operating condition of all security systems such as detectors, monitors, intruder alarm systems, and lighting upon receipt of an elevated threat advisory, and weekly thereafter until termination of the advisory.

33. Increase monitoring of network intrusion systems.

34. Identify additional business- and site-specific measures as appropriate.

35. Remind personnel of the reporting requirements for any unusual enterprise or control systems network activity and to be vigilant regarding suspicious electronic mail.

36. Conduct security awareness briefings for employees and on-site contractors.

37. Coordinate the security of critical facilities with neighboring organizations including other electricity sub-sector organizations and large customers.
38. 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.

39. Place all essential critical facility support personnel on alert.

40. 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.

41. Consider restricting parking around critical facilities and/or outside perimeter fence.

42. 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.

43. Enforce strict control of visitors and visitor vehicles entering critical facilities.

44. Consider postponing or canceling nonessential tours and visits.

45. When appropriate, contact suppliers and coordinate with combustible deliveries as necessary.

46. Perform a periodic inspection of site fuel storage and hazardous material facilities.

47. To the extent practical, coordinate critical facility security with adjacent facilities.

48. 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.

49. Coordinate any security related media releases with security, media relations, and management.

50. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

---

**Imminent Risk**

| 51 – 77 Items for consideration: |

**Definition:** The Imminent Risk 51-77 are actions recommended 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. This alert level may apply as a result of either an incident that occurs in North America outside of the electricity sub-sector, or a threat from an international, national, or regional incident.

**Response:** The recommended security measures are additional to those listed for the Elevated level 2. The duration 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 could cause hardship on personnel and could seriously impact facility business and security activities. Actions items to be considered at this alert level include:

51. Communicate the heightened alert level to all on-site personnel. The communication should include a request to be alert for unusual or suspicious behaviors or activities and to whom such should be reported. Ensure all on-site personnel are fully briefed on emergency procedures and emergency conditions as they develop.

52. 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.

53. Unless conditions dictate otherwise, open emergency center(s).

54. Account for all personnel at affected locations.

55. Implement security, incident response and business continuity plans as needed.

56. Security Managers should review security personnel requirements and augment with qualified personnel.

57. Consider deployment additional security personnel and resources to critical facilities.

58. Consider the release of nonessential personnel depending on the nature of the threat or incident.

59. Limit facility access to essential staff, visitors, and contractors.

60. Cancel or delay non-vital contractor work and services.

61. Allow deliveries from trusted vendors, contractors, suppliers by appointment only. Inspect all deliveries, to include packages and cargo. Require advance notice of deliveries and identification of drivers.

62. Inspect all bags, backpacks, purses, etc., prior to entering the facility.

63. Inspect all vehicles prior to gaining access to the facility.

64. Discontinue all tours and visitors.

65. Consider discontinuing mail and package deliveries to critical facilities or deliver to offsite locations for inspection or subsequent delivery.

66. Consider suspending maintenance work on essential equipment, except work that management determines to be emergency work and critical.
67. Continuously monitor or otherwise secure all entrances to critical service facilities. This step may include use of armed security personnel or law enforcement officers. Heavy equipment and storage material may be moved and used as barriers at closed entrances.

68. Erect barriers and/or obstacles to control vehicle traffic flow and protect the facility from attack by moving vehicles.

69. Identify and implement plans for any additional measures specific to the facility as appropriate based on available intelligence.

70. 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. Coordinate with local authorities regarding the closing of nearby public roads and facilities, if appropriate.

71. Where possible, restrict vehicle parking to 150 ft. from all critical areas and assets.

72. Limit network communications links to essential sites/users.

73. Review remote access for individuals and revoke any credentials that are not current and necessary.

74. Conduct daily security and awareness briefings for each shift relevant to security concerns of the alert or threat.

75. Participate in situation update briefings with government agencies, local law enforcement, and internal interdependent business units, as well as coordinate media releases or inquiries, and coordinate impacts to adjacent/nearby businesses or neighbors.

76. In the event of an actual incident affecting the Grid, Security Personnel should liaison with Grid Operations Personnel to ascertain the next potential affected site in the critical path.

77. Continue to monitor the situation and be prepared to de-escalate to a lower threat alert level.

Revision History:

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version Number</th>
<th>Reason/ Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 14, 2002</td>
<td>1.0</td>
<td>Issuance of the ESISAC-developed four-state threat condition model (ThreatCon Normal, Low, Medium, and High). Document titled, Threat Response.</td>
</tr>
<tr>
<td>Date</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>November 1, 2005</td>
<td>3.0</td>
<td>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, <em>Security Guideline – Physical Response</em>.</td>
</tr>
<tr>
<td>May 2013</td>
<td></td>
<td>Update Guideline and refresh of document, including the new Department of Homeland Security (DHS) and National Terrorism Advisory System (NTAS).</td>
</tr>
</tbody>
</table>

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](http://www.dhs.gov/dhspublic/display?theme=29). The DHS and NTAS 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.


Appendix A found below in this document has been developed for the possible use as a flip chart/checklist, produced in hard copy, and may be utilized at a local site.
RESPONSE GUIDELINES

PHYSICAL SECURITY

ITEMS FOR CONSIDERATION
RESPONSE GUIDELINES

1. Confirm normal security operating procedures are current, in place, and operational.
2. Provide training and updates for security staff and key personnel on all aspects of the response plan, as well as specific pre-planned operating standards and procedures.
3. Periodically issue workforce security awareness messages.
4. Train mail handling personnel and all employees handling mail directly on-site on the characteristics of suspicious mail or packages. Review response procedures for these items.
5. Brief on daily and threat related security topics at employee meetings to increase security awareness.
6. Provide recurring training of hazardous material, security, and emergency response personnel.
7. No person should be permitted access to the facility without proper authorization by authorized management.
8. Authorized persons will adhere to access control procedures and prevent tailgating or other unauthorized entry.
9. Identification badges, permanent or temporary are required for all individuals, including employees, contractors, and visitors.
10. Individuals or persons not possessing or displaying an identification badge should be challenged to determine their identity and reason for their presence. Appropriate action should be taken upon this determination.
11. Visitors should receive badges, be required to sign in, providing appropriate identification to verify their identity.
12. Annually audit electronic or other access programs for critical facilities to ensure proper access authorization.
13. Conduct routine maintenance and inspection of security equipment to ensure that it is in good working order.
14. Conduct routine security inspections and patrols of the facility and critical areas and components and report unattended of findings.
15. Conduct periodic security tabletop exercises with facility and or executive management as appropriate. Consider involvement of law enforcement as well as tours of facilities for familiarity of response.
16. Review and update all security, threat, cyber, business continuity, and disaster-recovery plans on an ongoing basis or at least once every year.

Baseline
RESPONSE GUIDELINES

17. Unusual or suspicious activities observed by personnel should be reported to local law enforcement, local management and security.

18. Identify critical facility long-term and short-term security measures as appropriate. Examples of security measures are:
   - Electronic security systems (fobs, alarms, cameras, access control, etc.)
   - Closing continuous perimeter and internal portals
   - Identify and secure all essential perimeter and internal portals and establish accountability
   - Physical barriers such as bollards or concrete barriers
   - Perimeter signage
   - Fence integrity
   - Lighting effectiveness
   - Security surveys
   - Vulnerability assessments
   - Availability of security resources – contract and proprietary
   - Law enforcement liaison (FBI, jurisdictional law enforcement agencies, Fusion Center, etc.)
   - Maintain essential spare parts for critical facilities

Baseline (cont)
RESPONSE GUIDELINES

19. Communicate the heightened alert level to all security staff and onsite personnel at the critical facilities. This should include vendors with routine deliveries. The communication should include a reminder to be alert for unusual or suspicious activities and details on whom it should be reported. Security staff at other, non-critical facilities also should be made aware of the increased threat level.

20. Inform local law enforcement agencies that the facility is at an elevated alert level, confirm communications methods to be utilized and advise them of the security measures being employed. Request that agencies increase the frequency of patrols at critical facilities.

21. Security personnel should review company security and incident response plans and procedures.

22. Review operational plans and procedures to ensure they are up to date. They should include the following:
   a. Security, fire, disaster recovery, fail-over plans, incident response plan, and business continuity plan.
   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 ensure operability, use, familiarity, and backup function as designed.

23. Review fuel source requirements.

24. Review vehicle search procedures.

25. Increase surveillance of critical areas and facilities.

26. Monitor and restrict all deliveries. Particularly deliveries of combustible materials such as kerosene, diesel fuel, and gasoline. Confirm delivery with receiving personnel. Request list(s) of anticipated deliveries of those essential to continued operations.

27. 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 the delivery is consistent with the paperwork).

28. Conduct random inspections of vehicles.

29. Ensure all gates, security doors, and security monitors are in working order, and that visitor, contractor, and employee access controls are enforced.

30. Evaluate the necessity of non-critical maintenance and capital project work that could affect facility security. Delay or reschedule this work as appropriate.

31. Increase lighting in facility buffer zones, if feasible.

Elevated Risk
RESPONSE GUIDELINES

31. 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.
32. Verify the operating condition of all security systems such as detectors, monitors, intruder alarm systems, and lighting upon receipt of an elevated threat advisory and proceed immediately to termination of the advisory.
33. Increase monitoring of network intrusion systems.
34. Identify additional business- and site-specific measures as appropriate.
35. Remain personnel of the reporting requirements for any unusual enterprise or control systems network activity and be vigilant regarding suspicious electronic mail.
36. Conduct security awareness briefings for employees and on-site contractors.
37. Coordinate the security of critical facilities with neighboring organizations.
38. 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.
39. Place all essential critical facility support personnel on alert.
40. 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.
41. Consider restricting parking around critical facilities and/or outside perimeter fence.
42. Where appropriate, ensure all gates and security doors are locked and monitored twenty-four hours a day, seven days a week, either electronically or by random patrol procedures.
43. Enforce strict control of visitors and visitor vehicles entering critical facilities.
44. Consider suspending or canceling nonessential tours and visits.
45. Where appropriate, contact suppliers and coordinate with combustible deliveries as necessary.
46. Perform a periodic inspection of site fuel storage and hazardous material facilities.
47. To the extent practical, coordinate critical facility security with adjacent facilities.
48. 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.
49. Coordinate any security-related media releases with security, media relations, and management.
50. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

Elevated Risk (cont.)
RESPONSE GUIDELINES

51. Communicate the heightened alert level to all on-site personnel. The communication should include a request to be alert for unusual or suspicious behavior or activities and to whom such should be reported. Ensure all on-site personnel are fully briefed on emergency procedures and emergency conditions as they develop.
52. 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.
53. Unless conditions dictate otherwise, open emergency centers.
54. Account for all personnel at affected locations.
55. Implement security, incident response and business continuity plans.
56. Security Managers should review security personnel requirements and augment with qualified personnel.
57. Consider deployment additional security personnel and resources to critical facilities.
58. Consider the release of nonessential personnel depending on the nature of the threat or incident.
59. Limit facility access to essential staff, visitors, and contractors.
60. Cancel or delay non-critical contractor work and services.
61. Allow deliveries from trusted vendors, contractors, suppliers by appointment only. Inspect all deliveries to include packages and cargo. Require identification online of deliveries and identification of drivers.
62. Inspect all bags, backpacks, purses, etc., prior to entering the facility.
63. Inspect all vehicles prior to gaining access to the facility.
64. Discourage all tours and visitors.
65. Consider discontinuing mail and package deliveries to critical facilities or deliver to offsite locations for inspection or subsequent delivery.
66. Consider suspending maintenance work on essential equipment, except work that management determines to be emergency work and critical.
67. Continuously monitor or otherwise secure all entrances to critical service facilities. This step may include use of armed security personnel or law enforcement officers.
68. Erect barriers and or obstacles to control vehicle traffic flow and protect the facility from attack by moving vehicles.
69. Identify and implement plans for any additional measures specific to the facility as appropriate based on available intelligence.
70. 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 offices of the decision as soon as practical. Coordinate with local authorities regarding the closing of nearby public roads and facilities, if appropriate.
71. Where possible, restrict vehicle parking to 150 ft. from all critical areas and assets.

Imminent Risk
RESPONSE GUIDELINES

72. Limit network communications links to essential sites/users.
73. Review access control for individuals and revoke any credentials that are not current and necessary.
74. Conduct daily security and awareness briefings for each shift relevant to security concerns of the alert or threat.
75. Participate in situational update briefings with government agencies, local law enforcement, and internal interdependent business units, as well as coordinate media releases or updates, and coordinate impacts to adjacent nearby businesses or neighbors.
76. In the event of an actual incident affecting the Grid, Security Personnel should liaise with Grid Operations Personnel to ascertain the next potential affected site in the critical path.
77. Continue to monitor the situation and be prepared to escalate to a lower threat alert level.

Imminent Risk (cont.)