THREAT ALERT SYSTEM AND PHYSICAL RESPONSE GUIDELINES FOR THE ELECTRICITY SECTOR

Definitions of Physical Threat Alert Levels

A Model for Developing Organization Specific Physical Threat Alert Level Response Plans

Version 2.0
October 8, 2002

Developed by
North American Electric Reliability Council
Critical Infrastructure Protection Advisory Group

Approved by
Board of Trustees

Goals

- Define Threat Alert Levels for all alerts issued by the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC) in cooperation with the National Infrastructure Protection Center (NIPC) or other government agencies. These Threat Alert Levels and Physical Response Guidelines, however, do not apply to facilities regulated by the Nuclear Regulatory Commission.
- Provide guideline examples of security measures that electric utility organizations may consider taking, based on the Alerts issued.
- Ensure that the application of these electricity infrastructure Alert Levels are appropriate based upon the threat information received by the Electricity Sector Information Sharing and Analysis Center from government sources, Electricity Sector participants, and other ISACs.
- Ensure threat information from the Telecom, Oil/Gas, Information Technology, and other sectors is included, as appropriate, in the formulation of a Threat Alert.
- Note that Threat Alerts could be issued for a specific geographical area, such as "Specific Region Only," or "Specific City Only," or by category, such as "Specific Type of Facility."

Threat Alert Level Definitions

ES-Physical-Green (Low)

ES-Physical GREEN Applies when no known threat exists of terrorist activity or only a general concern exists about criminal activity, such as vandalism, which warrants only routine security procedures. Any security measures applied should be maintainable indefinitely and without adverse impact to facility operations. This level is equivalent to normal daily operations.

ES-Physical-Blue (Guarded)

ES-Physical BLUE Applies when a general threat exists of terrorist or increased criminal activity with no specific threat directed against the electric industry. Additional security measures are recommended, and they should be maintainable for an indefinite period of time with minimum impact on normal facility operations.

ES-Physical-Yellow (Elevated)

ES-Physical YELLOW Applies when a general threat exists of terrorist or criminal activity directed against the electric industry. Implementation of additional security measures is expected. Such measures are anticipated to last for an indefinite period of time.

ES-Physical-Orange (High)

ES-Physical ORANGE Applies when a credible threat exists of terrorist or criminal activity directed against the electric industry. Additional security measures have been implemented. Such measures may be anticipated to last for a defined period of time.

ES-Physical-Red (Severe)

ES-Physical-RED Applies when an incident occurs or credible intelligence information is received by the electric industry indicating a terrorist or criminal act against the electric industry is imminent or has occurred. This condition may apply as a result of an incident in North America outside of the Electricity Sector. Maximum security measures are

necessary. Implementation of such measures could cause hardship on personnel and seriously impact facility business and security activities.

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 an exhaustive or all-inclusive list of possible security measures. The intent is to help define the scope for measures each organization may implement for its specific Alert Level Response Plans, based on its very specific requirements. Not all measures are applicable to all organizations. An organization may decide to re-order the sequence of some measures it deems appropriate to its environment and responsibilities. It also is expected that most organizations may need to develop additional, specific security measures.

ES-Physical-Green (Low)

1. Normal security operating standards and procedures.
2. Occasional workforce awareness messages or tabletop exercises, as appropriate.
3. All Security, Threat, and Disaster Recovery Plans should be routinely reviewed and updated. Recommend an annual review as a minimum.

ES-Physical-Blue (Guarded)

4. Work force awareness messages to be alert to; unusual activities and whom to report such activities.
5. Review operational plans and procedures and ensure they are up-to-date, to include:
   A. Security, Threat, Disaster Recovery, and Fail-Over plans
   B. Other Operation Plans as appropriate, i.e., transmission control procedures
   C. Availability of additional security personnel
   D. Availability of medical emergency personnel
   E. Review all data and voice communications channels to assure operability, user familiarity, and backups function as designed
   F. Review fuel source requirements

ES-Physical-Yellow (Elevated)

6. Implement measures 1-5, if they have not already been implemented.
7. Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and employee access control are enforced.
8. Notify critical and on-call personnel.
9. Establish/assure communications with law enforcement agencies
10. Identify additional business/site specific measures as appropriate.

ES-Physical-Orange (High)

11. Implement measures 1-10, if they have not already been implemented.
12. Review need to revise plans in measure 3, based on current intelligence, and include additional instructions as appropriate to the Security/Threat Plans.
13. Place all critical and on-call personnel on alert, consider holding tabletop exercises.
14. Enforce safe zones around facilities per Security Plan.
15. Ensure all gates and security doors are locked and actively monitored either electronically or by “random walk-by procedures.”
16. Implement Enhanced screening procedures for:

A. Anyone entering the facility
B. All deliveries and packages

17. Contact and coordinate with fuel suppliers, as necessary.
18. Inspect site fuel storage and HAZ-MAT (hazardous material) facilities.
19. Increase liaison with law enforcement, medical emergency services, and other entities.
20. Coordinate critical facilities security with neighbors:
    A. Virtual neighbors such as other utility organizations
    B. Physical facility neighbors
21. Consider emergency utility operations procedures appropriate to available threat intelligence.
22. Media releases should be reviewed with Security/Alert Level Coordinator prior to release.
23. Review plan for returning to Threat Level-YELLOW, BLUE OR GREEN status.
24. Additional business/site specific measures as appropriate.

ES-Physical-Red (Severe)

25. Implement measures 1-24, if they have not already been implemented.
26. Send non-essential personnel home, per business/site specific procedures.
27. Stop all non-alert related tours and visitors.
28. Consider having medical emergency personnel on-site, if possible.
29. Continuously monitor or otherwise secure all entrances and critical service facilities, such as substations, etc. This step may include use of armed security personnel.
30. Stop all mail and package deliveries directly to site.
31. Inspect all vehicles entering site.
32. Ensure all on-site personnel are fully briefed on emergency procedures.
33. Establish frequent communications with all appropriate law enforcement agencies for two-way updates on threat status.
34. Review plan for returning to Threat Level-ORANGE, YELLOW, BLUE or GREEN status.
35. Additional business/site specific measures as appropriate.