# THREAT ALERT SYSTEM AND CYBER RESPONSE GUIDELINES FOR THE ELECTRICITY SECTOR

## Definitions of Cyber Threat Alert Levels

## A Model for Developing Organization Specific Cyber 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 Information Systems and Services (Cyber) Threat Alert Levels 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 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 entities may consider taking, based on Cyber Alert Levels issued.
- Ensure that the electricity infrastructure Cyber Threat Alert Levels are consistent with the threat information received by the NERC from Government sources and other ISACs.
- Assure that threat information from the Telecom, Oil/Gas, Information Technology, and other Sectors is included as appropriate in the formulation of a Cyber Threat Alert Level.
- Note that Cyber Threat Alert Levels could be issued (for example) for a specific computer platform or a communications protocol or service, such as "Windows 2000" or "SCADA Communications."

## Threat Alert Level Definitions

**ES-Cyber-GREEN (Low)**

ES-Cyber-GREEN condition applies when there is no known threat of cyber attack or only a general concern about hacker activity that warrants only routine security procedures. Any cyber security measures applied should be maintainable indefinitely and without adverse impact to business or expenses. This may be equivalent to normal daily conditions.

**ES-Cyber-BLUE (Guarded)**

ES-Cyber-BLUE condition applies when there is a general threat of increased cyber (hacker intrusions, viruses, etc.) activity with no specific threat directed toward the electric industry. Additional cyber security measures may be necessary, and if initiated they should be maintainable for an indefinite period of time with minimum impact on normal business or expenses.

**ES-Cyber-YELLOW (Elevated)**

ES-Cyber-YELLOW condition applies when a general threat exists of disruptive cyber activity is directed against the electric industry. Implementation of additional cyber security measures is expected. Such measures are anticipated to last for an indefinite period of time.

**ES-Cyber-ORANGE (High)**

ES-Cyber-ORANGE condition applies when a credible threat exists of disruptive cyber activity directed against the electric industry. Additional cyber security measures have been implemented. Business entities need to be aware that corporate resources will be required above and beyond those required for normal business or expenses.

**ES-Cyber-RED (Severe)**

ES-Cyber-RED Condition applies when an incident occurs or credible intelligence information is received by the electric industry indicating a disruptive cyber attack

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

## Cyber Response Guidelines for the Threat Alert Levels

The following are examples of security measures to be considered at each cyber threat level. This is not an exhaustive or all-inclusive list of possible security measures. The intent is to provide a scope of measures that each organization may implement for their specific threat response plan, based upon their own specific requirements. Not all measures are applicable to all organizations. Some organizations may decide to re-order the sequence of some measures, as they perceive appropriate to their environment and responsibilities. It is also expected that most organizations may perceive the need to develop additional, specific security measures to meet their requirements.

It is also recognized that some measures might not always be necessary or applicable against a particular threat. Therefore, when developing your specific response plan, it is recommended you do so with consideration as a checklist of all the possible security measures you might choose to initiate, based on the specific threat information available.

**ES-Cyber-Green (Low)**

1. Have an emergency plan for IT operations:
   A. Ensure all business critical information and information systems (including applications and databases) and their operational importance are identified.
   B. Ensure all points of access and their operational necessity are identified.
2. On a continuing basis, conduct normal security practices. For example:
   A. Conduct education and training for users, administrators, and management.
   B. Ensure an effective password management program is in place.
   C. Conduct periodic internal security reviews and external vulnerability assessments.
   D. Conduct normal auditing, review, and file back-up procedures.
   E. Ensure effective virus protection scanning processes are in place.
   F. Confirm the existence of newly identified vulnerabilities and test and install patches as available.
   G. Periodically review and test higher Threat Alert Level actions and IT recovery plans.
3. Maintain law enforcement liaison-e.g. local FBI, InfraGard, RCMP

**ES-Cyber-Blue (Guarded)**

4. Implement measures 1-3 if not already implemented.
5. Communicate work force awareness messages to be alert and who to report unusual cyber activities to.
6. Review security and operational plans and procedures and ensure they are up-to-date.

**ES-Cyber-Yellow (Elevated)**

7. Implement measures 1-6 if not already implemented.
8. Increase level of auditing, review, and critical file back-up procedures.
9. Conduct internal security review on all critical systems.
10. Increase review of intrusion detection and firewall logs.

11. More frequent checks of cyber security communications for software vulnerability.
12. Identify additional business/site specific measures as appropriate.
13. Increase frequency of measure 3 – include additional instructions as appropriate to your Cyber Alert Level Response Plan.

**ES-Cyber-Orange (High)**

14. Implement measures 1-13, if not already implemented.
15. Conduct immediate internal security review on all critical systems.
16. Determine staffing availability for backup operations and provide notice.
17. Consider increasing physical access restrictions to computer rooms, communications closets, and critical operations areas.
18. Consider account access restrictions-temporarily disable non-critical accounts.
19. Consider delaying scheduled, routine maintenance or non-security sensitive upgrades.
20. Media releases should be reviewed with Cyber Alert Level Coordinator prior to release.
21. Review plan for returning to Alert Advisory Level-Yellow, Blue or Green.
22. Additional business/site specific measures as appropriate.

**ES-Cyber-Red (Severe)**

23. Implement measures 1-22, if not already implemented.
24. Consider 7/24 emergency tech support staffing.
25. Consider continuous 7/24 monitoring of intrusion detection and firewall logs.
26. Consider continuous 7/24 monitoring of cyber security communications for latest vulnerability information. Contact software vendors for status of software patches and updates.
27. Consider reconfiguring information systems to minimize access points and increase security.
28. Consider rerouting mission-critical communications through unaffected system.
29. Consider disconnecting non-essential network access.
30. Consider alternative modes of communication and disseminate new contact information, as appropriate.
31. Consider activation of the company emergency management team/procedures.
32. Actively monitor communications with all appropriate law enforcement and cyber security agencies for two-way updates on threat status.
33. Review plan for returning to Advisory Alert Level- Orange, Yellow, Blue and Green.
34. Additional business/site specific measures as appropriate.