



North American Electric Reliability Council Standards & Guidelines Working Group

Usage Guide for the CIPC Guidelines Template

Introduction to the Usage Guide:

This guide is a companion document to the NERC CIPC Security Guidelines template. As such it describes:

- What a guideline document should look like
- How each section of the guideline should be filled in

The reference numbers in the comment 'balloons' in the template correspond to the section numbers in the usage guide.

The template was drafted using Microsoft Word 2002 and its 'Comment' feature. Once a guideline is drafted, one may choose to delete all the comment balloons for ease of reading.

Drafting Guide:

General Guidelines:

1) Standard vs. Guideline Contents:

In general, the NERC Standards document "What's", and the NERC Guidelines should offer possible "How's" either through documenting the pluses and minuses of various options or laying out the steps of a defined process. NERC guidelines should also be of a specific nature to the utility industry and not generic IT documents or be conceptual in nature. Their primary use is to put them in the hands of the industry personnel to go DO something.

2) Guideline Tone of Writing:

In general, the NERC Guidelines should not have too many must's, shall's or will's in their writing. If these words must be used, a serious review needs to be made to see if the document being drafted is a standard.

Title and Header Section:

1) Guideline Title:

Provide a short, representative title for the guideline. If it does not fit in one line, the title may be too long. Consider shortening it.

2) Document ID:

Indicate the document ID number unique to CIPC guidelines. The ID numbers are controlled by the NERC CIPC co-ordinator. (Note: This item is a suggestion by S Harada at this time).

3) Version Number: *Rv*



North American Electric Reliability Council Standards & Guidelines Working Group

The version number will also be controlled by the NERC CIPC co-ordinator. Enter the number here.

4) Effective From Date:

Indicate the date when this version of the guideline becomes effective. Express it in an ISO standard date format: e.g., 2005 Apr 12 or 2005-04-12.

5) Effective To Date:

Indicate the date when this version of the guideline ceases to be in effect. A guideline will be automatically given a default service life of two years from the "Effective From" date. Express it in an ISO standard date format: e.g., 2005 Apr 12 or 2005-04-12.

However, there may be specific expected events or circumstance to shorten the service life. The Chair of the Standards and Guidelines Working Group (SGWG) will schedule reviews of the guidelines coming close to the end of their service life.

Body of the Guideline:

6) Preamble (a.k.a. the `Boiler Plate`):

This is a standard statement indicating the intended usage of the NERC CIPC guidelines. Leave these statements as they are and do not change.

7) Introduction:

Introduce the subject and, if appropriate, provide a brief background to the guideline being drafted for the NERC CIPC.

8) Purpose:

State what the guideline is designed to accomplish.

9) Scope of Application:

Indicate the scope of the guideline application which could be expressed in terms of:

- Personnel Types
- Organization Types
- Plant/Asset Types
- System Types
- Process Types
- Others

10) Guideline Statement or General Guideline:

Provide a summary statement on the guideline.



North American Electric Reliability Council Standards & Guidelines Working Group

(Question to SGWG members: Do we need this section at all times? For a simple guideline, can one dive right into the guideline details? We have Introduction and Purpose leading up to this section.

11) **Guideline Details:**

Provide the details of the guideline. As the content is added, keep in mind the following:

- Consistency with other NERC policies, standards, guidelines, procedures, FAQ and other documents to the best of your knowledge.
- Sufficient detail of information given, or too much detail.
- Comprehensiveness of the subject area
- Logical organization of the details

12) **Definitions:**

There are two types of definitions for CIPC standards and guidelines:

- **Common (or Global) Definitions:**
Those definitions that are referred to from multiple documents. These are defined outside individual standards and guidelines and made available through NERC CIPC Glossary of Terms. The definitions belonging to this set should be only `referred to` from the standards and guidelines and should not be `imbedded` in individual documents.
- **Local Definitions:**
Those definitions that are referred to only in this specific standard or document. These are defined in the Definition Section of the document.

Supplementary Data:

13) **Related Documents:**

Provide a list of related documents. The list should follow the following rules:

- Other NERC documents: indicate the title and the document ID
- WEB Link: embed a web link as close to the referenced document as possible.
- Books and Articles; follow a standard biblio format

14) **Revision History:**

For each revision, enter date, the proposed version number, and a brief summary of the revision.

This section may be effectively used by drafting teams to control draft versions. However, when the drafting is done and the version endorse, the only revision history remains would be the key changes in the latest version.



North American Electric Reliability Council
Critical Infrastructure Protection Committee

Guideline Title: _____

NERC	Guideline (DRAFT)
Document ID_[S2]:	Version No_[S3]:
Effective From Date_[S4]:	Effective To Date_[S5]:

Preamble:

_[S6]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:

_[S7]First paragraph of this section.

Purpose:

_[S8]First paragraph of this section.

Scope of Application:

_[S9]First paragraph of this section.

Guideline Statement:

_[S10]First paragraph of this section.

Guideline Details:

_[S11]First paragraph of this section.

Revise



North American Electric Reliability Council Critical Infrastructure Protection Committee

Definitions:

[S12]The following definitions apply in the guidelines:

Definition-1:	Description of Definition-1
Definition-2:	Description of Definition-2
Definition-3:	Description of Definition-3
Definition-n:	Description of Definition-n

Related Documents and Links:

[S13]First paragraph of this section.

Revision History:

[S14]

Date	Version Number	Reason/Comments
yyyy/mm/dd		Reason 1.

[S1]Usage Guide Reference 1)
[S2]Usage Guide Reference 2)
[S3]Usage Guide Reference 3)
[S4]Usage Guide Reference 4)
[S5]Usage Guide Reference 5)
[S6]Usage Guide Reference 6)
[S7]Usage Guide Reference 7)

[S8]Usage Guide Reference 8)

[S9]Usage Guide Reference 9)
[S10]Usage Guide Reference 10)

[S11]Usage Guide Reference 11)

[S12]Usage Guide Reference 12)
[S13]Usage Guide Reference 15)
[S14]Usage Guide Reference 16)

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

NERC	Guideline
Guideline Title: Vulnerability and Risk Assessment	Version: 1.1
Revision Date:	Effective Date: TBD

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.

Purpose:

A vulnerability and risk assessment helps identify critical facilities and functions as well as the risks and vulnerabilities associated with those facilities and functions. Such an assessment also helps identify countermeasures to mitigate threats and allows asset owners to make rational decisions about the level of protection needed.

Each company must assess the need to conduct a Vulnerability and Risk Assessment within the context of its operating environment.

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 company.

Each company is free 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 them less critical than others.

From an industry wide perspective, a critical facility or function may be defined as any facility/function or combination thereof which, 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.

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

Guideline Statement:

This guideline provides a broad overview as well as reference materials for the electricity sector in the area of “Vulnerability and Risk Assessment” for facilities and functions identified as critical.

Table of Contents:

Guideline Detail:

Vulnerability analyses and risk assessments provide established methods of prioritizing the criticality of assets (or the impact of the loss of the asset), threats, and countermeasure strategies. A structured risk assessment process allows for the documentation of these assets, threats, and countermeasure strategies by subject matter experts based on their judgments and assumptions. The final product is a broad set of priorities, both physical and cyber, that contribute to the protection of critical facilities or functions.

Using a vulnerability and risk assessment survey tool may be useful for the following:

- prioritizing critical assets and identification of vulnerabilities
- prioritizing risks and their priorities, and
- prioritizing countermeasures.

Cyber as well as physical security should be assessed as part of this process.

There are a number of risk/vulnerability assessment models some of which are fairly generic in nature while others are more complex or even directed toward specific types of assets such as dams or transmission facilities. Some are very resource intensive while others rely more on the collective judgment of the asset owner. Included in the reference materials for this guideline are white papers prepared in 2005 by the Department of Energy and the NERC Critical Infrastructure Protection Committee Risk Assessment Working Group that include a description of some of the available methodologies used in the electric sector as well as an approach developed by the Edison Electric Institute (EEI) Security Committee.

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

An Outline of Analytical Risk Management Steps

The following is an outline of a risk management process primarily used to assess vulnerabilities and to assist in the development and prioritization of countermeasures to mitigate the vulnerabilities identified. There are many models, and companies should choose the model that best fits their operational environment. There are four steps to the risk management process.

1. Identification of assets and loss impacts.
 - a. Determine the critical assets that require protection using the definition provided earlier in the guideline as well as a team approach involving operational, security, and other subject matter experts.
 - b. Identify possible undesirable events (both natural and manmade) and assess their impacts (consequences.)
2. Assess the level of risk associated with each critical facility/function:
 - a. Contact the nearest FBI field office as well as state and local law enforcement agencies to determine if they are aware of any threats to a specific facility or class of facilities.
 - b. Industry sources such as NERC, EEI, APPA, NRECA, and others can provide an assessment of threats to the electric industry as a whole or to individual segments based on their ongoing interactions with the Department of Homeland Security and other federal agencies.
 - c. The above referenced associations sponsor periodic meetings and conferences to discuss security related matters and provide a perspective on the nature of threats as well as security practices.
 - d. Based on those discussions as well as the entity's own judgment and experience:
 - Estimate the likelihood of an attack by a potential adversary
 - Estimate the likelihood that specific vulnerabilities will be exploited

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

3. Prioritize the assets based on the nature of the identified threat(s) and the consequence of loss.

4. Identification and analysis of vulnerabilities:
 - a. This can be done using one or more of the approaches described in the papers referenced in the appendix or using any other assessment method that the entity determines is best suited to its operations and the nature of the risk identified through its analysis.

 - b. Identify potential vulnerabilities related to specific assets or undesirable events. (This does not mean every conceivable vulnerability but those that are determined to have the most adverse consequences and/or the entity determines is a logical target for exploitation.)

 - c. Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.

 - d. Estimate the degree of vulnerability relative to each asset.

5. Identification of countermeasures, their costs and trade-offs.
 - a. Identify potential countermeasures to reduce the identified vulnerabilities.

 - b. Estimate the cost of the countermeasures.

 - c. Conduct a cost-benefit and trade-off analysis.

 - d. Prioritize options and recommendations for senior management.

 - e. Document the process, findings, and implementation actions resulting from the assessment.

6. There is a wide range of mitigation measures that can be considered as part of the process but are sometimes overlooked as they are part of normal utility operations practices. They include:
 - a. Coordinate security response requirements with law enforcement officials at the appropriate federal, regional, and local levels to

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

assure good communication and coordination in protecting the critical infrastructure facilities.

- b. Develop an emergency management response process to reduce or mitigate impacts of a loss of electric supply or deliverability (see guideline on emergency planning).
- c. Prepare a mutual assistance agreement or understanding at the appropriate local, state, or regional level to support response, repair, and restoration activities for the disrupted critical infrastructure facility.

Consider interdependencies among infrastructures when evaluating the consequences of a cyber or physical security incident. An incident in one infrastructure can cascade to cause failures in other infrastructures.

Also consider coordinating contingency response plans with other infrastructure entities and sectors to assure coordination during emergencies.

Exceptions:

Certified Products/Tools:

Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Threat Response
 - Emergency Plans
 - Continuity of Business Processes
 - Communications

Version 1.1
Approval Date: TDB

Security Guideline:
Vulnerability and Risk Assessment
Page 5 of 6

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.nerc.com>

— *Threat Alert Levels and Physical Response Guidelines*, NERC, November, 2001, <http://www.nerc.com>

— *Threat Alert Levels and Cyber Response Guidelines*, NERC, March 2002, <http://www.nerc.com>

Revision History:

Date	Version Number	Reason/Comments

CIPC members are requested to review the technical content of this guideline.
Formatting of this guideline will be completed prior to any balloting by CIPC.

THREAT ALERT SYSTEM AND PHYSICAL RESPONSE GUIDELINES FOR THE ELECTRICITY SECTOR

Definitions of Physical Threat Alert Levels

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

Version 2.1

TBD

Developed by
North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Committee

Approved by
~~NERC Board of Trustees~~

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.

Goals

- Communicate the Threat Alert Levels¹ (Alert) for all alerts issued by the NERC Electricity Sector Information Sharing and Analysis Center (ESISAC) in cooperation with the National Infrastructure Coordination Center (NICC) or other government agencies.
NOTE: These Threat Alert Levels and Physical Response Guidelines do not apply to facilities regulated by the Nuclear Regulatory Commission.
- Provide examples of security measures that electric utilities 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 ESISAC from government sources, Electricity Sector participants, and other sources.
- Ensure threat information from the Telecom, Oil/Gas, Information Technology, and other sector ISACs is included, as appropriate, in the formulation of a Threat Alert.
- Note that Threat Alerts may be issued generically or for a specific geographical area, such as “Specific Region Only,” or “Specific City Only,” or by industry or facility specific category such as “Electric Generating Station, Substation etc.”

MATERIAL INCORPORATED IN NEXT SECTION

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. The intent of this guideline is to help in defining the measures each utility may implement for its specific Alert Level Response Plans, based on the nature of the threat and that utilities specific requirements. Not all measures are applicable to all utilities. A utility may decide to re-order the sequence of some measures it deems appropriate to its facilities and corporate responsibilities. It also is expected that most utilities may need to develop additional, specific security measures beyond the scope of those listed below.

ES-Physical-Green (Low)

The utilities Alert Level Response Plans are enacted at 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, which warrants only routine security procedures. Any security measures applied should be maintainable indefinitely and without adverse impact to company operations. This level is equivalent to normal daily operations.

1. Normal security operating standards and procedures are in place and operational.
2. Train security staff and key personnel on all aspects of the Plans, as well as specific preplanned operating standards and procedures.

¹ The Office of the Secretary of the United States Department of Homeland Security is responsible for initiating a change in the national/regional/sector specific area Threat Alert Level. The information is conveyed to the ESISAC via the National Infrastructure Coordination Center (NICC) as well as other government agencies.

3. All visitors should be approved before being allowed entry into a critical facility or access to a critical system.
4. Individuals not known or otherwise approved should be stopped to determine identity and reason for presence and appropriate action taken (i.e. issued a badge, removed from the property).
5. Routine maintenance and inspection of electronic security equipment should be conducted so that equipment is maintained in good working order at all times.
6. Periodic posting or release of workforce awareness messages or the conducting of tabletop exercises, as appropriate.
7. All Security, Threat, and Disaster Recovery Plans should be routinely reviewed and updated to assess their ability to identify terrorist threats and vulnerabilities. Recommend an annual review as a minimum.
8. Any unusual or suspicious activity observed by critical facility personnel or contractors should be reported to security or facility management.
9. Security topics should be incorporated into 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 HazMat response, security, and other emergency response personnel.
12. Identify additional critical facility long-term and short-term security measures as appropriate. Examples of possible additional security measures are:
 - Electronic Security Systems
 - Closing non-essential perimeter and internal portals
 - Physical barriers such as bollards or Jersey (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

ES-Physical-Blue (Guarded)

The Guarded Threat Alert Level applies when there exists a general threat of terrorist or increased criminal activity with no specific threat directed against the electric industry. The recommended security measures are additional to those listed for Low. The Guarded level should be maintainable for an indefinite period of time with minimum impact on normal company operations.

13. The heightened security level should be communicated to all personnel and contract workers at critical facilities and to the security staff at all other utility owned facilities. The communication should include a reminder to be alert for unusual or suspicious activities and to whom such activities should be reported.
14. Monitor all deliveries, particularly deliveries of combustibles such as start-up fuel, diesel fuel, gasoline, etc.
15. 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. Review all data and voice communications channels to assure operability, user familiarity, and backups function as designed
16. Providing the public law enforcement agencies with any information that would strengthen its ability to act appropriately.

ES-Physical-Yellow (Elevated)

The Elevated Threat Alert Level applies when there exists a general threat of terrorist or criminal activity directed against the electric industry. The recommended security measures are additional to those listed for Low and Guarded. Such measures are anticipated to last for an indefinite period of time.

17. Increase the surveillance of critical locations.
18. Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and employee access controls are enforced.
19. Notify critical and on-call personnel.
20. Establish/assure ongoing internal and external communications and coordinate the utilities action plans with local law enforcement agencies.
21. Review operational plans and procedures and ensure they adequately address the terrorist threat associated with the reason for the Elevated Threat Alert Level. Identify additional business/site specific measures as appropriate.

ES-Physical-Orange (High)

The High Threat Alert Level applies when there exists a credible threat of terrorist or criminal activity directed against the electric industry on an international, national or regional basis. The recommended security measures are additional to those listed for Low, Guarded, and Elevated. Such measures are anticipated to last for a defined period of time.

22. The heightened security level should be communicated 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.
23. Use communications channels with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations and other emergency management agencies responsible for response to the critical facility to assess the nature of any threats to the facility/company.
24. Review related emergency action plans based on current intelligence and consider activation of alternate 'back up' operational control and office work centers as appropriate.
25. Place all essential critical facility support personnel on alert.
26. 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.
27. Consider restricting parking around critical facilities.
28. Where appropriate, ensure all gates and security doors are locked and actively monitored 24/7 either electronically or by random patrol procedures.
29. If feasible, identity of delivery personnel should be verified and a general inspection of deliveries conducted, (i.e. is paperwork in order and external appearance of deliveries consistent with paperwork).
30. Enforce strict control of visitors and visitor vehicles entering critical facilities.
31. Consider postponing or canceling non-essential tours and visits.
32. When appropriate, contact suppliers and coordinate with combustible deliveries as necessary.
33. Perform a periodic inspection of site fuel storage and HAZ-MAT (hazardous material) facilities.
34. To the extent practical, coordinate critical facility security with adjacent facilities, (neighboring facilities, businesses, etc.)
35. 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 these essential units and equipment.
36. Coordinate security related media releases with security, media relations, and management. Take additional measures as deemed appropriate.
37. Monitor conditions and be prepared to escalate to a higher level or deescalate to a lower level.

ES-Physical-Red (Severe)

The Severe Threat Alert Level applies when an incident occurs or credible intelligence information indicates a terrorist or criminal act against any segment of the North America electric industry is imminent or has occurred. As conditions warrant, the threat level may be applied on an international, national or regional basis. This Alert Level may also apply as a result of an incident in North America that is outside of the Electricity Sector. During this period, maximum-security measures will be recommended and all security measures, defined for Low to Elevated, shall be enacted as appropriate to each utility. The alerts duration will be defined by the incident, but 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.

38. The heightened security level should be communicated 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.
39. Contact law enforcement and other government agencies to determine the nature of the threat and its applicability to system and business operations.
40. Unless conditions dictate otherwise, open emergency center(s).
41. Account for all personnel at critical facilities, at locations that were affected by any incident, or were mentioned in the threat to the industry.
42. Unless circumstances dictate otherwise, deploy additional security resources to critical facilities.
43. Consider the release of non-essential personnel depending on the nature of the threat or incident.
44. Discontinue all tours and visitors.
45. Consider the discontinuance of mail and package deliveries to critical facilities.
46. Consider suspending maintenance work on essential equipment, except that determined to be emergency work and critical by management. (See above Threat Level – is this needed)
47. 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.
48. Inspect all vehicles entering critical facilities.
49. Identify and implement plans for any additional measures specific to the facility as appropriate based on the threat intelligence.
50. If feasible, close public access areas such as boat ramps, recreation areas etc. If these facilities are part of FERC licensed projects, inform the FERC regional office of the decision as soon as practical.
51. Continue to monitor the situation and be prepared to de-escalate to a lower threat alert level condition.

Summary

The recommended actions defined for each Physical Threat Alert Level provides a framework that utilities can refer to in assessing the actions that might be appropriate to their individual facilities. The suggested levels of increased security measures with each successive Threat Alert Level will aid utilities in responding to threats and inform them of possible actions that will safeguard employees, assure coordination with local, State, and Federal law enforcement and officials, inform the public about preparations, and provide all with necessary information and direction. Each utility is encouraged to perform a terrorist-based risk assessment of their critical operational and business facilities and to develop an Physical Alert Level Plan that will define the individuals actions to be taken and the coordination that would be appropriate with neighboring utilities, businesses served by that utility, and other agencies as noted in this guideline.