NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Implementation Guidance for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

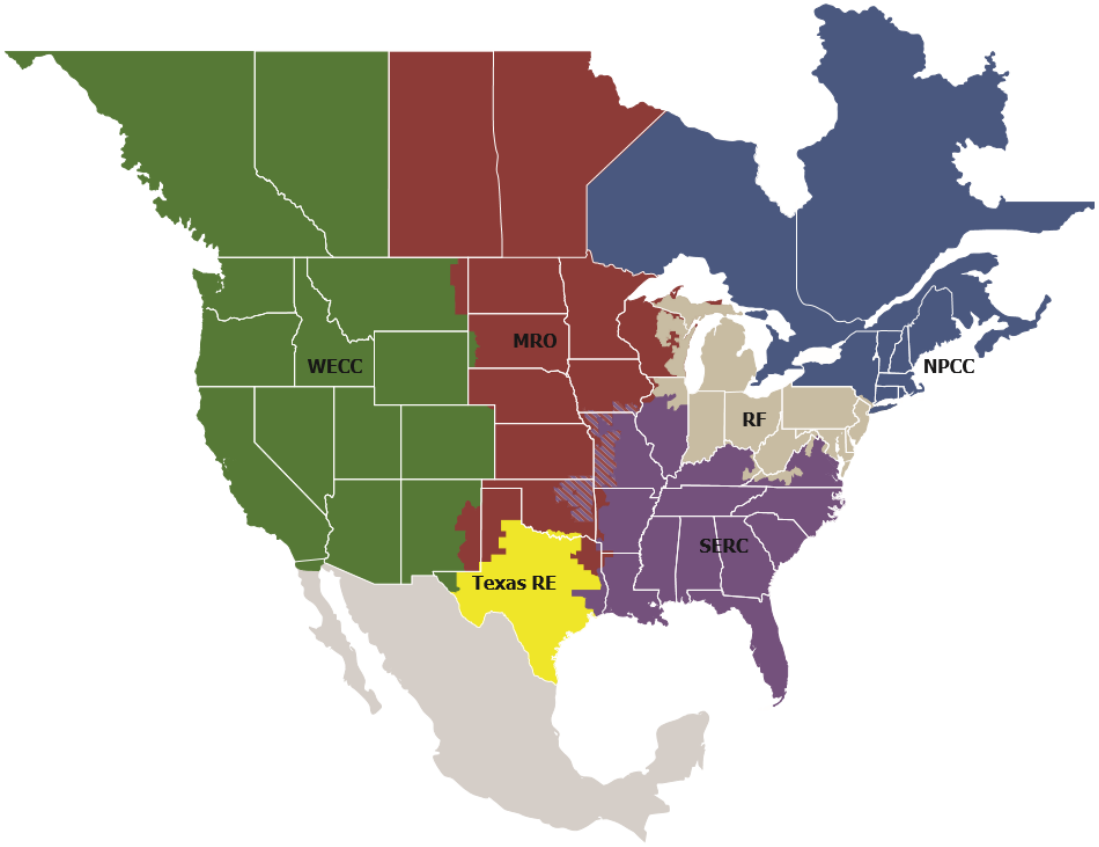
Preface iii
Introduction iv
Requirement R1 1
General Considerations for Requirement R1 1
Implementation Guidance for R1 1
Requirement R2 2
General Considerations for Requirement R2 2
Implementation Guidance for R2 2
Requirement R3 3
General Considerations for Requirement R3 3
Implementation Guidance for R3 3
Requirement R4 4
General Considerations for Requirement R4 4
Implementation Guidance for R4 4
Requirement R5 5
General Considerations for Requirement R5 5
Implementation Guidance for R5 5
Requirement R6 0
General Considerations for Requirement R6 0
Implementation Guidance for R6 0
Apendix 1: Implementation Guidance for CIP-004-6 2

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-004-X. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for the modifications to CIP-004-X.

[1] NERC's Compliance Guidance Policy

Requirement R1

General Considerations for Requirement R1

None

Implementation Guidance for R1

None

Requirement R2

General Considerations for Requirement R2

None

Implementation Guidance for R2

The Responsible Entity has the flexibility to define the training program, and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles, or responsibilities at the discretion of the Responsible Entity.

Requirement R3

General Considerations for Requirement R3

None

Implementation Guidance for R3

None

Requirement R4

General Considerations for Requirement R4

None

Implementation Guidance for R4

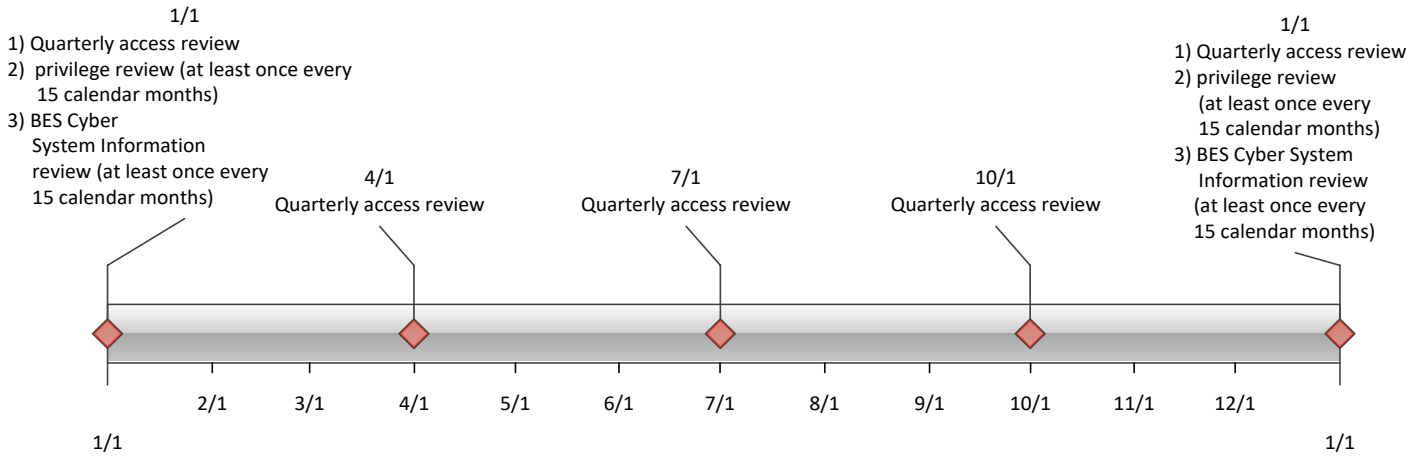
Consider including the person or persons empowered by the Responsible Entity to authorize access in the delegations referenced in CIP-003-8.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

Quarterly reviews can be achieved by comparing individuals actually provisioned access against records of individuals authorized for provisioned access. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

Entities can more efficiently perform the 15-calendar-month review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed.

An example timeline of all the reviews in Requirements R4 and R6 is included below.



Requirement R5

General Considerations for Requirement R5

None

Implementation Guidance for R5

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

If an entity considers transitioning a contracted individual to a direct hire, an entity should consider how they will meet the evidentiary requirements for Requirements R1 through R4. If evidence for compliance with Requirements R1 through R4 cannot be provided, the entity should consider invoking the applicable sub-requirements in Requirement R5 for this administrative transfer scenario. Entities should also consider including this scenario in their access management program, including a higher-level approval to minimize the instances to which this scenario would apply.

Requirement R6

General Considerations for Requirement R6

None

Implementation Guidance for R6

This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the 15-calendar-month verification in Requirement R6. The person reviewing should be different than the person provisioning access.

Entities may choose not to provision access, or provision temporary rather than persistent access, for authorized users. In other words, an authorized individual does not have to have any access provisioned, but all provisioned access must be authorized.

An entity can choose to give an authorization to access any BCSI, or they can have authorizations for specific storage locations or types of BCSI, if they so choose.

While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint

where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program. In this case, the review required in Requirement R6 Part 6.2 should still be performed, and the revocation required in Requirement R6 Part 6.3 could consist of removing the individual's name from the authorized list at the time of termination or upon review when it is determined the individual no longer has a need.

Entities can more efficiently perform the 15-calendar-month BCSI review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. For an example timeline to perform the 15-calendar-month BCSI review, refer to the graphic in the *Implementation Guidance for R4* section.

An example where a termination action in Requirement R5 Part 5.1, satisfies Requirement R6 Part 6.3, would be the Responsible Entity revoking an individual's means of unescorted physical access and Interactive Remote Access (e.g., physical access card, virtual private network, Active Directory user account). By revoking both physical and electronic access, the individual could ultimately not have access to BES Cyber System Information. The Responsible Entity should still revoke access that is manually provisioned (e.g., local user account, relay, site area network server, cloud based BCSI that is not tied to an active directory account).

Appendix 1: Implementation Guidance for CIP-004-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale sencan be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:
Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:
The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Requirement R3:
Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check.

Requirement R4:
To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

(i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts.

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The list of provisioned individuals can be an automatically generated

account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

Requirement R5:
Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.