NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-7

August 2020

RELIABILITY | RESILIENCE | SECURITY




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

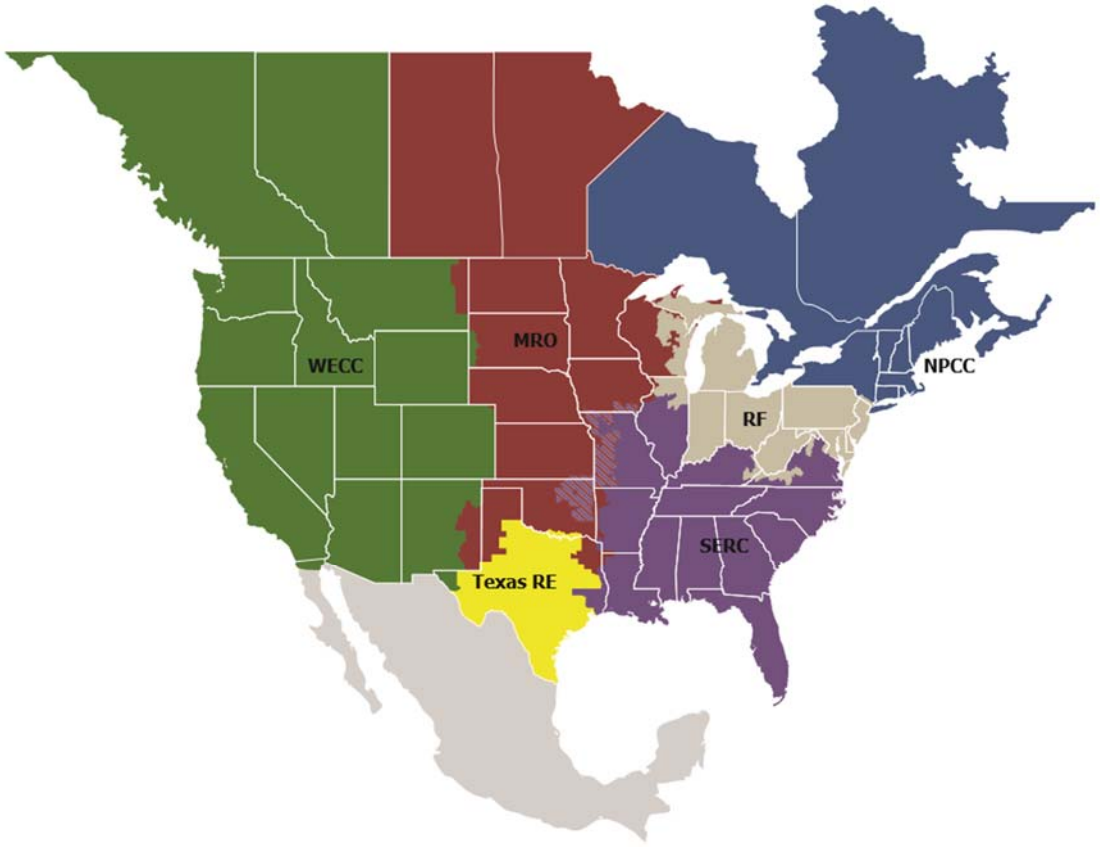
Table of Contents

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 document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the intent of the Standard Drafting Team (SDT) in drafting the requirements. This Technical Rationale and Justification for CIP-004-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving and initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-004-7 to require Responsible Entities to implement specific controls in Requirement R6 for provisioning, periodic review, and revocation of access related to BES Cyber System Information.

New and Modified Terms Used on NERC Reliability Standards

Proposed Modified Terms

None

Proposed New Terms

None

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

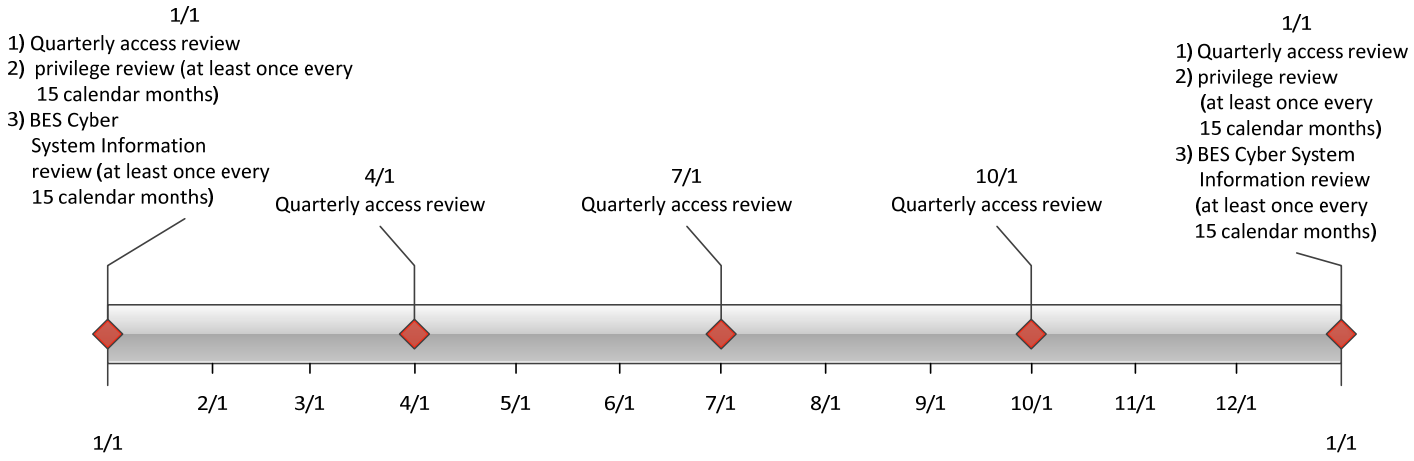
Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, the SDT intends that access authorization and provisioning be performed by different people where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

An example timeline of all the reviews in Requirement R4 is included below.



If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement 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.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information access management program with specific controls for access authorization, periodic review of provisioned access, and access revocation related to BES Cyber System Information, which, if accidentally or maliciously misused, could negatively impact the reliable operation of the Bulk Electric System. Authorization ensures only individuals who have a need are authorized for provisioned access to BES Cyber System Information. The periodic review ensures access is still required and has been provisioned appropriately and accurately. Revocation of access when individuals are terminated helps prevent inappropriate disclosure of sensitive information.

Requirement R6 shifts the focus to authorizing provisioned access to BES Cyber System Information itself. This is important when considering vendor services in which BES Cyber System Information is outside of the Responsible Entity's direct control.

Methods to document and track authorization for access where provisioning of access is a prerequisite of being able to obtain and/or use the BES Cyber System Information.

The SDT intends that access requirements do not apply to BES Cyber System Information where no specific provisioning mechanisms are available or feasible, or where provisioning is not specific to provisioning access to BES Cyber System Information. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room. There will likely be no specific provisioning of access to BES Cyber System Information on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BES Cyber System Information is only temporarily or incidentally located or stored there. The previous concept of designated storage locations was meant to exclude these locations. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BES Cyber System Information that may be located there. In these cases, access authorization, periodic review of provisioned access, and access revocation related to BES Cyber System Information would not be required. However, BES Cyber System Information in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required in CIP-011-3.

The SDT clarified the intent of addressing BES Cyber System Information as opposed to the BES Cyber System with associated applicable systems, which may contain BES Cyber System Information; the Applicability column has added language to specify BES Cyber System Information that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Requirement 6.1 has been drafted to ensure access authorization occurs only for individuals who have a need for provisioned access to BES Cyber System Information. Authorization should be considered to be a

grant of permission by a person or persons empowered by the Responsible Entity to perform such grants. Authorization for provisioned access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys). For BES Cyber System Information in physical format, physical access is provisioned to a physical storage location. For BES Cyber System Information in electronic format, electronic access is provisioned to an electronic system's front-end interface regardless of the geographical or physical location of the server or storage device or to individual encrypted files. Provisioning physical access to a physical location or storage device that contains electronic BES Cyber System Information is not considered provisioning access to electronic BES Cyber System Information. However, the Responsible Entity's information protection program and relevant information protection controls should be considered to prevent unauthorized access to BES Cyber System Information as required in CIP-011-3.

The SDT also intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R4, Part 4.1). Authorization for access to BES Cyber System Information must still be based on necessity of the individual performing a work function. Documentation showing the authorization should still have some justification of the business need included. To ensure proper segregation of duties, the SDT intends that access authorization and provisioning be performed by different people where possible.

Requirement 6.2 has been drafted to ensure the Responsible Entity reviews provisioned access privileges to BES Cyber System Information at least every 15 calendar months. The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges for BES Cyber System Information are the minimum necessary to perform their work function.

The SDT intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R4, Part 4.4). The 15-calendar-month review of BES Cyber System Information privilege is still in place to ensure an individual's associated privileges to BES Cyber System Information are the minimum necessary to perform their work function (i.e., least privilege). This involves determining the specific roles with BES Cyber System Information (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access to BES Cyber System Information does not assume any specific software, and it 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 BES Cyber System Information privilege review on individual accounts.

Requirement 6.3 ensures an individual who is involved in a termination action has their access to BES Cyber System Information promptly revoked. Access revocation (also referred to as "deprovisioning of access") is still understood to mean a process with the result that electronic access to BES Cyber System Information is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Access can only be revoked where access has been provisioned. Revoking access prevents any further access from that point in time onwards. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Responsible Entities should still consider the ramifications of deleting an account might include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The SDT intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R5, Part 5.3). The requirement to revoke access to BES Cyber System Information at the time of the termination action still includes procedures showing revocation of access to BES Cyber System Information concurrent with the termination action. This requirement also still recognizes the timing of the termination action might vary depending on the circumstance.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the Technical Rationale 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 compliance guidance can be found in a separate Implementation Guidance document for this standard.

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

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks

associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

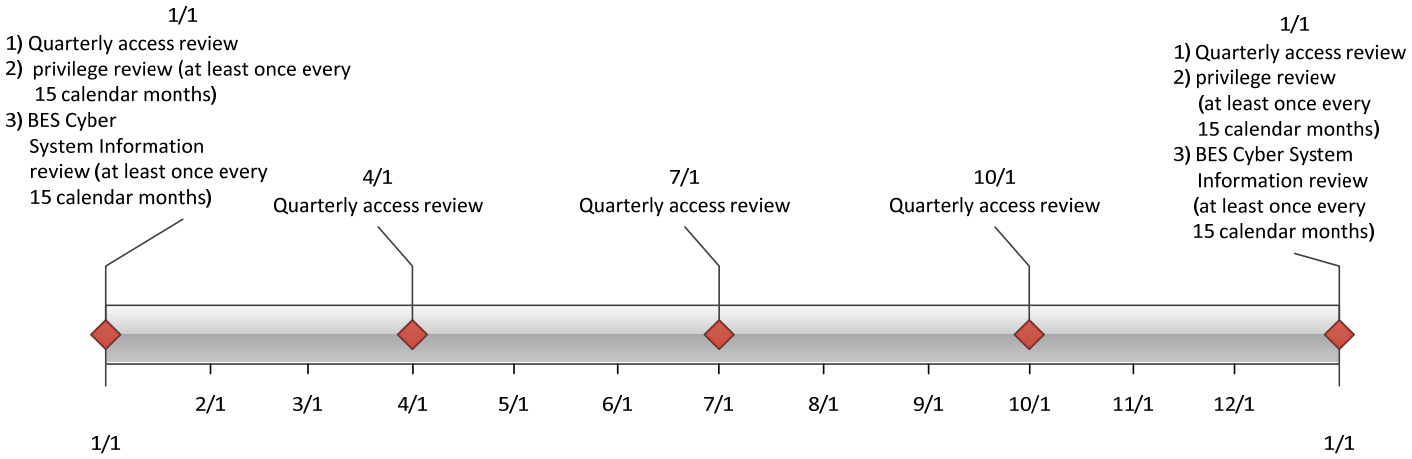
Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

An example timeline of all the reviews in Requirement R4 is included below.



If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement 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.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. 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 focus of this

requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).