NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 and R5 to CIP-004-X R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	CIP-004-X, Requirement R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium]*	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes clarification on the specific elements within an access management program that need to be implemented. In addition, a definition of what constitutes BCSI access was included in the parent R6 requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	[Time Horizon: Same Day Operations and Operations Planning].	
CIP-004-6, Requirement R4, Part 4.1.3 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	**CIP-004-X, Requirement R6, Part 6.1, 6.1.1, and 6.1.2** Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	The modified requirement language includes a shift from authorizing access to designated storage locations, to authorizing the provisioned access to BCSI. The Note was included to specify the type of access to be authorized (6.1), verified (6.2) and revoked (6.3).
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	**CIP-004-X, Requirement R6, Part 6.2, 6.2.1, and 6.2.2.** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is still needed.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R5, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	**CIP-004-X, Requirement R6, Part 6.3** For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.
CIP-004-6, Requirement R5, Part 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**CIP-004-6, Requirement R5, Part 5.3** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	This Part was renumbed from 5.4 to 5.3 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. The reference within the Part was changed to just Part 5.1.
CIP-004-6, Requirement R5, Part 5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the	**CIP-004-6, Requirement R5, Part 5.4** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating	This Part was renumbed from 5.5 to 5.4 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. This is a renumbering change only, no changes were made to the Part's requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	