NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-2

BES Cyber System Information (BCSI)-related access management requirements were moved from CIP-004-6, Requirements R4 and R5, to CIP-011-2, Requirement R1. In addition, new requirements have been implemented to mitigate risks associated with BCSI and off-premises vendor services.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.1 Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Added requirement language for Responsible Entities to identify designated BCSI storage locations, whether physical or electronic, along with BCSI, which was already required.
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	CIP-011-3, Requirement R1, Part 1.2 Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use and disposal.	Established a stand-alone requirement for authorization of access to BCSI based on need, except for CIP Exceptional Circumstances. This change helps to consolidate all BCSI-related requirements under one CIP Standard. This sub-requirement was carried over from CIP-004-6, Requirement R4, Part 4.1.3. Added the lifecycle element “disposal” to the

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
		requirement to complement actions taken in CIP-011-2, Requirement R2.
CIP-004-6, Requirement R4, Part 4.1.3 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.3 Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Access to designated storage locations for BES Cyber System Information moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus changed from access to designated storage locations to access to BES Cyber System Information.
N/A	CIP-011-3, Requirement R1, Part 1.4 (NEW) Process(es) to identify, assess and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and	New CIP-011-3 requirement which is similar to the cyber security risk assessment required as part of CIP-013 Requirement R1. This new requirement is intended to focus risk analysis on potential vendors that will be hosting Responsible Entity's BCSI in the cloud.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	
CIP-004-6, Requirement R4, 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-011-3, Requirement R1, Part 1.5 For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Next calendar day termination actions for those with access to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus of termination actions changed from access to designated storage locations to access to BES Cyber System Information.
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	CIP-011-3, Requirement R1, Part 1.6 Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity	15-month entitlement reviews to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
determines are necessary for performing assigned work functions.	determines are necessary for performing assigned work functions.	Focus of verification changed from designated storage locations to BES Cyber System Information.
N/A	CIP-011-3, Requirement R2 R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.1 (NEW) Where applicable, develop a key management program to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation,

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.2 (NEW) Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	New CIP-011-3 requirement that requires implementation of controls that ensure the separation of duties and organizational independence between the programs used to restrict the ability to obtain BCSI from those programs used to restrict the ability to use BCSI.
CIP-011-2, Requirement R2, Part 2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems"	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber	Combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Asset data storage media shall be sanitized or destroyed.	In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 Requirement R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.
CIP-011-2, Requirement R2, Part 2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	As above. CIP-011-2, Requirement R2, Part 2.2 was combined into CIP-011-3, Requirement R3, Part 3.1.