Mapping Document
Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-2

The modifications made to requirements within CIP-011-2 are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use). In addition, new requirements have been implemented to mitigate risks associated with BCSI access when utilized in 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 Method(s) to identify BCSI.	Requirement language simplified.
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 protect and securely handle BCSI.	Requirement revised to a focus around the implementation of controls that prevent the unauthorized access to BCSI (concurrent ability to obtain and use) in storage, transit, and use.
N/A	CIP-011-3, Requirement R1, Part 1.3 (NEW) When the Responsible Entity engages vendor services to store, utilize, or analyze	This new CIP-011-3 requirement is similar to the cyber security risk assessment required as part of CIP-013 Requirement R1, however it is intended to focus the risk assessment

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	BCSI, implement risk management method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	on the security controls used by the vendor to manage the environment that will be used to host Responsible Entity's BCSI.
N/A	CIP-011-3, Requirement Part 1.4 (NEW) When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	This new CIP-011-3 requirement is intended to address any risks identified under CIP-011-3, Requirement R1, Part 1.3 through the implementation of technical controls to prevent unauthorized logical access to BCSI.