NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-X

The modifications made to requirements within CIP-011-X are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use).

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection Program*.	**CIP-011-X, Requirement R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to Applicable Systems that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program.*	Parent CIP-011-X Requirement R1 language modified to sharpen focus on protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems, which may contain BCSI.
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	**CIP-011-X, Requirement R1, Part 1.1** Method(s) to identify BCSI.	Requirement language simplified.

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
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-X, Requirement R1, Part 1.2** Method(s) to protect and securely handle BCSI to mitigate the risks of compromising confidentiality.	Requirement revised to broaden the focus around the implementation of controls that mitigate the risks of compromising confidentiality in any state, not just storage, transit, and use.