# CIP-007-7 Technical Rationale

## Project 2016-02: Modifications to CIP Standards

### CIP-007-7 R1

The original technical rationale for CIP-007-6 Requirement R1 described the existence of Requirement R1 as being needed "…to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports." The reasoning remains the same for Requirement R1 with the new objective language "to mitigate the risk posed by uncontrolled logical and physical connectivity." The changes in Requirement R1 language continue the move from Cyber Asset up to the BES Cyber System and supports the secure configuration implemented within CIP-010-3 Requirement R1.

CIP-007 Requirement R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment.

### CIP-007 R1 Part 1.1

The move to logical connectivity supports the proliferation of additional connectivity options found in modern technology stacks such as virtualization. With SAN connectivity over Fiber Channel delivering storage to virtualized systems without the use of IP or a "network," the limitation of network based controls becomes more clear. Additionally, the connectivity of a local hypervisor based configuration manager to the VM likewise does not go through a "network accessible port" in the strict sense.

By moving the control to "logical connectivity" the requirement can be applied in both the original "logical network accessible port" model as well as in the virtualized system to apply access controls to the network and storage "fabric" and hypervisor supporting a virtualized BES Cyber System.

### CIP-007-7 R2

The original technical rationale for CIP-007-6 Requirement R2 included the intent "to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets." This intent was determined to logically fit within the intent of CIP-010-2 R3 associated with vulnerability assessment and management. Accordingly, the SDT moved the related requirements from CIP-007-6 Requirement R2, with modifications supporting virtualization, to CIP-010-4 Requirement R3 Parts 3.5 and 3.6.

The SDT is including a replacement requirement related to controlling software that is allowed to execute on applicable BES Cyber Systems with the inclusion of the objective "to mitigate the risk posed by unmanaged software". This clarifies one of the implied requirements of the original CIP-007-6 Requirement R2 for a list of software, and supports the secure configuration implemented within CIP-010-4 Requirement R1.

## CIP-007 R2 Part 2.1

The inclusion of the objective in Requirement R2 Part 2.1, “to allow only essential software execution” further clarifies the intent of CIP-007 Requirement R2 to limit what software can execute on a system. This requirement helps ensure that entities control software execution, which limits the attack vectors, and limits the scope of required software vulnerability management efforts in CIP-010-3 R3 Parts 3.5 & 3.6.