NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance pending submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Implementation Guidance for Reliability Standard CIP-005-7

~~May~~ July 2020

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

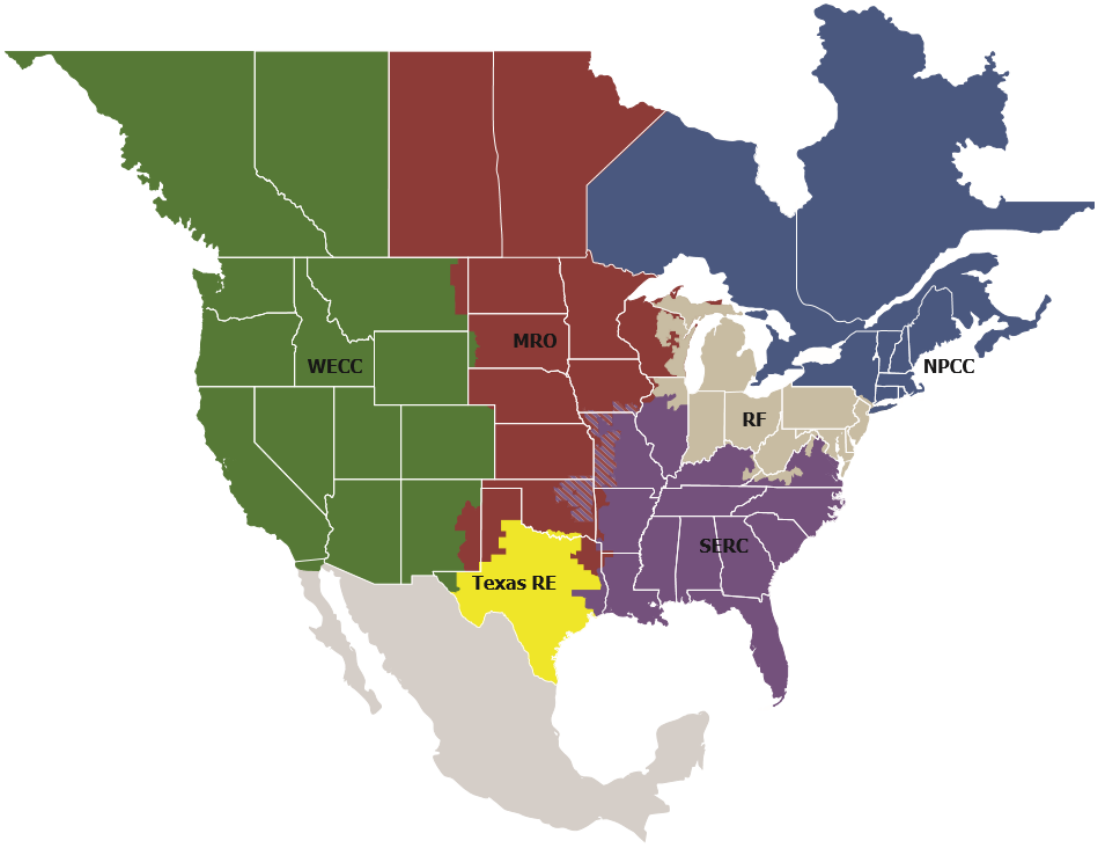
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The Standards Project 2019-03 – Cyber Security Supply Chain Risks Standards Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-005-7. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP-005-7.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

[1] NERC's Compliance Guidance Policy

Requirement R3

The 2019-03 SDT added Requirement 3 Vendor Remote Access Management for EACMS and PACS and created new Requirements ~~along with adding EACMs and PACs to the Applicable Systems column for Requirement P~~parts 3.1 and 3.2 to meet FERC order 850 and the NERC Supply Chain Risk report. ~~-~~If an entity allows remote access to their EACMS and PACS the method to determine authenticated ~~for~~ vendor-initiated remote ~~access~~ connections ~~would be~~is documented and the ability to disable that remote ~~access~~ connection ~~would be~~is required. ~~-~~For example, if an entity utilizes its corporate remote access solution to allow remote ~~access~~ connection into its PACS, the entity would need to document the authenticated remote ~~access~~ connection ~~method, and~~method and develop a process to ~~remove~~ terminate such connections~~access~~ after authentication. ~~-Removing~~ Some examples of how an entity might terminate ~~access~~ these connections may be as simple as, but are not limited to actions like disabling a token or certificate for ~~that~~a vendor ~~user~~ account(s), ~~or~~ suspending or deleting ~~that user's~~the ~~-~~vendor account(s) in Active Directory ~~account~~, blocking the ~~IP~~ vendor's IP range, or physically disconnecting ~~pulling~~ a network cable.

~~Since~~ Intermediate Systems (a subset of EACM~~CSs~~) ~~are~~ use is not a requirement for remote access to other EACMS, ~~lessesning~~lessening the ~~s the~~ potential of the recursive requirement ~~-~~("hall of mirrors") ~~issue is lessened (see above examples for terminating remote vendor connections).~~ ~~-~~However, if an Entity uses the same system (Intermediate System for example) for remote connections and access into both their BES Cyber Systems and their EACMS, the process of ~~disabling remote access~~ terminating vendor-initiated remote connections begins after the entity has determined, through authentication, that this particular connection attempt should not be allowed. ~~becomes tricky. Since the standard requires the removal of remote access to EACMS how can that be accomplished on the EACMs itself, the "hall of mirror" effect?~~ For this example, assume the Entity is using a jump host as its Intermediate System with multifactor and Active Directory authentication. When the vendor~~user~~ attempts the remote access connection~~session~~, the jump host will present both the Active Directory login screen as well as the multifactor access portal. ~~-~~The Entity could choose to disable the Active Directory account, disable the multifactor account or both. Any of those methods disable~~d~~ the vendor's~~user's~~ ability to make a connection. ~~"access" the EACMs.~~ The remote access vendor~~user~~ will attempt to "connect" with the EACMS~~s~~ however, after unsuccessful authentication the connection attempt ~~session~~ will be terminated.~~not allow "access" without the authentication methods being enabled, thus effectively not allowing remote access to that EACMS.~~ This scenario ~~shows~~ illustrates a method to ~~not~~ disallow vendor-initiated ~~-~~remote access while eliminating the recursive requirements ("hall of mirror") issue.

Where an entity strictly prohibits vendor-initiated remote access as a function of policy, the entity should consider the following to provide reasonable assurance of conformance to that policy, noting the policy itself can become the documented method:

1. Document whether the policy contains provisions to allow deviations to accommodate emergency situations, as well as the process to handle or approve those policy deviations, and how vendor-initiated remote connection termination would be handled if needed during those emergencies.
2. An Entity could identify internal controls to periodically verify vendor-initiated remote access is prohibited within system configurations. Some examples may include, but are not limited to:
    a. Leveraging periodic access reviews conducted in support of CIP-004-6 Requirement R4 and CIP-007-6 Requirement R5 to provide ongoing reasonable assurance that vendor-initiated remote access is prohibited as expected.
    b. Leveraging periodic inventory reviews that may be associated to annual CIP-002-5.1a Requirement R2 to assess BES Cyber System classifications and architecture to provide supporting records that vendor-initiated remote access needs and configurations were reviewed and confirmed to be in alignment with policy expectations.

c. Leveraging periodic rule set or access list configuration reviews that may be performed in support of CIP-005-7 and verification of implemented controls for EAP, ESP, and as Intermediate System implementation to provide additional assurance that vendor-initiated remote access is prohibited as expected.

d. Leveraging periodic configuration change management reviews performed in support of CIP-010-4~~3~~ Requirement R2 to assess BES Cyber Systems and unexpected (or potentially unauthorized) changes to baseline configurations that could lead to the introduction of vendor-initiated remote access to provide additional assurance that vendor-initiated remote access is prohibited as expected.

e. Leveraging periodic cyber vulnerability assessments performed in support of CIP-010-4~~3~~ Requirement R3 to assess BES Cyber System connectivity characteristics, interface and protocol configurations, and unexpected (or potentially unauthorized) physical connections to provide additional assurance that vendor-initiated remote access is prohibited as expected.

f. Provisions within the Responsible Entity's remote access management program or processes detailing internal controls and technology used to monitor for unauthorized access to provide additional assurance that the introduction of vendor-initiated remote access could be detected and reverted/revoked if established in violation of policy.

Staff augmentation presents another example of vendor remote access; however, this method provides less risk as other vendor remote access. The process involved requires an entity to complete all the CIP-004 tasks for the vendor in the same rigor as with an employee (training, PRA, etc.) and provide the vendor with an entity managed device to facilitate the remote access. This type of vendor remote access should be managed the same as an entity manages employee remote access.

Implementation Guidance for CIP-005-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale can be found in a separate Technical Rational document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Requirement R1:

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked

Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.