NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
CIP Version 5 Transition Program

Vendor Access Management

Version: November 23, 2015

This document is designed to convey lessons learned from NERC's various CIP version 5 transition activities. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Purpose

The purpose of this Lesson Learned is to provide discussion points for Responsible Entities to consider when developing processes for managing vendor access to BES Cyber Systems.

Background

This lesson learned provides approaches used by Implementation Study participants.[1] Under Reliability Standard CIP-004-6, Cyber Security - Personnel & Training, Responsible Entities are required to ensure that all individuals (employees, contractors, and vendors) who are authorized for unescorted physical and/or electronic access to BES Cyber Systems meet all of the applicable requirements. While the content of this lesson learned focuses on CIP-004-6, Responsible Entities may also need to consider how other standards requirements (e.g., CIP-005-5, CIP-006-6, CIP-011-2) could be applicable to vendors and the responsibilities the vendors may be performing or managing for the Responsible Entities. Figure 1 provides examples of types of vendor responsibilities and the standards Responsible Entities may need to consider.

Guidance

The Responsible Entity may choose to have a written contract with the vendor that incorporates specific language to address and delineate the vendor's responsibilities to meet the requirements of the CIP version 5 standards.

The Responsible Entity may consider the following areas to be addressed in the contract with the vendor.

[1] Ref. Implementation Study Final Report http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf

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

- Understand the compliance responsibility and accountability for entities that delegate the performance of reliability related tasks to a third party[2]
- Identification of the specific standard requirements the vendor must meet to be in compliance
- Non-disclosure agreement containing appropriate protective language
- Language to address contractor access to applicable BES Cyber System Information
- Language to specifically address the contractor's need for electronic access and/or unescorted physical access to applicable BES Cyber Systems
- Language to address the contractor designating a person(s) to be responsible for compliance with contract requirements

The Responsible Entity will need to determine if they will require the vendor to take the Responsible Entity's NERC CIP training or allow the vendor to take the vendor's own version of the training. If the vendor is permitted to take their own version of the training, the Responsible Entity should take into consideration how to document and ensure that the vendor's training fully meets all of the applicable requirement parts in CIP-004-6, Requirement R2. The Responsible Entity should determine how to adequately document that each of the vendor's employees who will access the Responsible Entity's systems have successfully completed the training before the Responsible Entity authorizes access. This could include developing a process to ensure that each of the vendor's employees who have a business need for continued authorized access to BES Cyber Systems completes the training at least once every 15 calendar months.

The Responsible Entity should determine if they will require the vendor to use the same background check service provider(s) that the Responsible Entity has reviewed and approved to ensure that the background check criteria meets all of the personnel risk assessment requirements in CIP-004-6, Requirement R3. If the vendor is permitted to use their own background check service provider(s), the Responsible Entity should consider how to document and ensure that the vendor's background search process fully meets all of the requirements of CIP-004-6, Requirement R3. The Responsible Entity should consider how to adequately document that each of the vendor's employees has met the requirements of CIP-004-6, R3 before authorizing access.

The Responsible Entity should determine if they will use the same physical and electronic access management and access revocation processes for vendor employees that are used for their own employees to meet the requirements in CIP-004-6, Requirement R4 and Requirement R5. If the Responsible Entity chooses not to use the same processes for vendor employees that are used for their own employees, the Responsible Entity should consider how they will document processes specific to vendor employees to authorize access. In addition, the Responsible Entity may find it useful to develop specific vendor processes to remove the vendor employee's unescorted physical and electronic access. It may be useful for the Responsible Entity to identify their point-of-contact to the vendor to enable prompt communication of information related to vendor employee changes such as terminations and transfers.

If the Responsible Entity allows vendors to access their BES Cyber Systems remotely, that access will need to be securely managed in accordance with the CIP version 5 standards. One study participant chose to utilize a WebVPN portal customized to allow electronic access only to specific devices. The WebVPN portal presents a customized

[2] Ref. NERC Compliance Public Bulletin #2010-004, Guidance for Entities that Delegate Reliability Tasks to a Third Party Entity http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance%20Process%20Bulletin%202010-004_v2_.pdf

webpage that utilizes a Secure Sockets Layer (SSL) VPN from the vendor's computer to the Responsible Entity's firewall. The connection is proxied by the Responsible Entity's firewall which functions as an Intermediate System. This allows the vendor to securely access only authorized BES Cyber Systems without directly connecting to the Responsible Entity's network. The secure portal requires two-factor authentication and the Responsible Entity remains in control of the remote access by retaining the token assigned to the vendor, thus requiring the vendor to call the Responsible Entity to receive the current token code that must be used to gain access to the portal. This allows the Responsible Entity to be aware of all remote access by the vendor.

If the Responsible Entity allows a vendor to perform reliability tasks or manage/operate the Responsible Entity's BES Cyber Systems, the Responsible Entity still remains accountable for documenting compliance with the requirements. One approach the Responsible Entity may choose to consider is additional contract language to document expectations to meet the CIP version 5 standards requirements. For example, the Responsible Entity could include contract provisions that require assessments or reviews to be conducted by the Responsible Entity or acceptable third parties. The Responsible Entity could also require additional specifications for network equipment to address patching considerations or ports and services documentation. The continuum provides examples of various vendor responsibilities and the associated standards to consider when developing processes for managing vendor access to BES Cyber Systems.

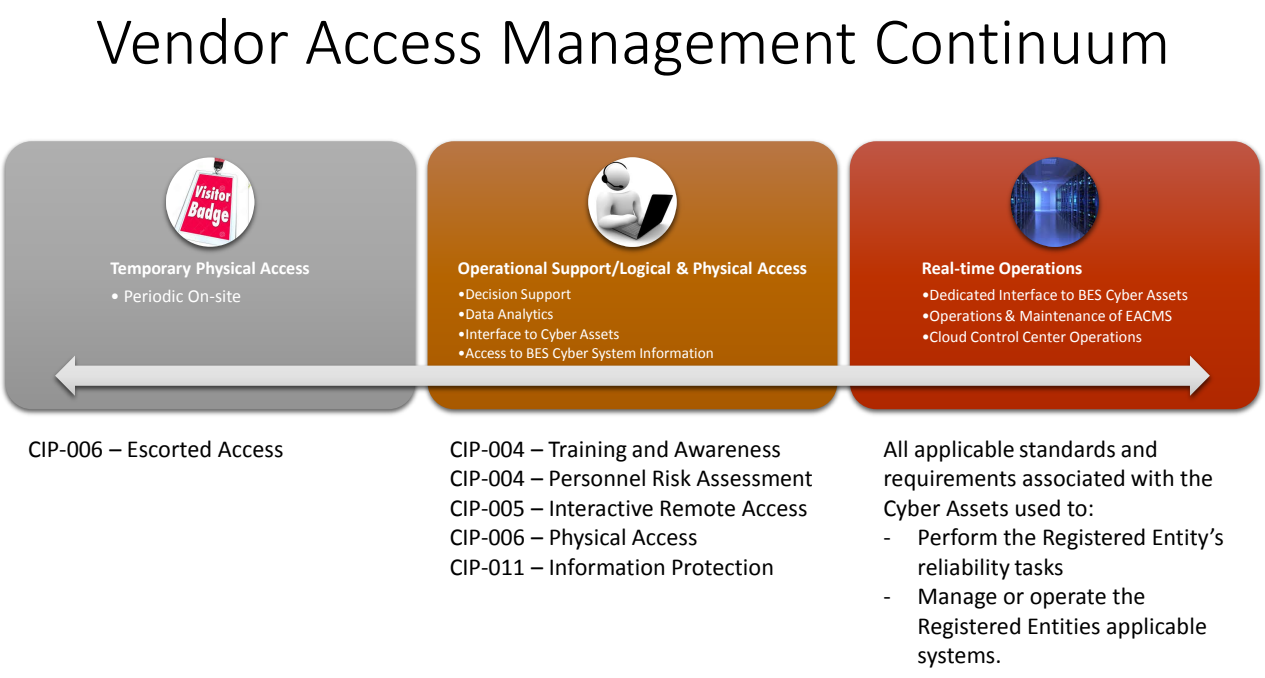

Figure 1: Example of Vendor Access Management Considerations