Vendor Remote Access

Implementation Guidance for CIP-005-6 R2 Requirement Parts 2.4 and 2.5

Version 1.0

Approved: November 6, 2017

This document was submitted to NERC for consideration as compliance "Implementation Guidance" on 11/8/17. NERC will review and post a decision on its website.

Document Approval			
Ken Keels Director, Practices and Initiatives		Version 1.0	Date Approved: 11/6/2017

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve transmission reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Open Distribution

Contents

Revisions

Date	Version	Notes
10/16/2017	1.0	Original issue

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Regarding vendor remote access, the Commission states in Order No. 829 the following:

> Therefore, we recognize that the current CIP Reliability Standards do contain certain controls addressing the risks posed by vendor remote access, as noted by commenters. However, the current CIP Reliability Standards do not require monitoring remote access sessions or closing unsafe remote connections for either vendor Interactive Remote Access and vendor machine-to-machine remote access. Accordingly, we determine that vendor remote access is not adequately addressed in the approved CIP Reliability Standards and, therefore, is an objective that must be addressed in the supply chain management plans directed in this final rule.[1]

Vendor remote access risks are addressed with additions to CIP-005-6 Requirement 2; specifically the addition of requirement parts 2.4 and 2.5.

The North American Transmission Forum (NATF) developed this document to outline considerations and potential approaches for implementing the requirements in CIP-005-6 R2 parts 2.4 and 2.5, depending on the Responsible Entity's[2] individual facts and circumstances. The examples provided herein are not the only approaches for complying with CIP-005-6, rather, Responsible Entities may choose alternative approaches that better fit their situations.[3]

---

[1] Order No. 829, paragraph 80

[2] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

[3] As stated in the November 5, 2015, Compliance Guidance Policy: "Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [footnote omitted] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard. The ERO Enterprise's endorsement of an example means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." *Available at:* http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

CIP-005-6 Requirement R2

Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 – Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Plan ning and Same Day Operations].

General Considerations for R2

CIP-005-6 Requirement R2 has been expanded to address remote access management, not just Interactive Remote Access as in previous versions. Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine (or system-to-system) vendor remote access (P. 51). The objective is to mitigate potential risks to a Responsible Entity's BES Cyber Systems from a compromise at a vendor who initiates an active remote access session with those systems.

Vendor remote access sessions contain two subcategories or types of remote access:

- Interactive Remote Access. This is the term as defined in the NERC glossary and is the user initiated type of remote access.
- System-to-system access (also referred to at times as "machine-to-machine"). While not a defined term in the NERC glossary, this type of remote access involves a BES Cyber System or PCA inside one of the Responsible Entity's ESPs that has an application or programmatic level interface with a system outside of the ESP and used by a vendor either onsite or at a remote vendor location. This type of vendor remote access is typically used for data acquisition.

The vendor remote access requirements concentrate the Responsible Entity's efforts in two areas:

- Awareness of active vendor remote access sessions (requirement part 2.4)
- Ability to disable active vendor remote access sessions (requirement part 2.5)

A simplified vendor remote access reference model is included in Appendix A for your reference.

Implementation Guidance for Requirement R2

The number of process(es) and their content may depend on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many processes as necessary to meet its needs.

Requirement Part 2.4

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

Implementation Guidance for Requirement Part 2.4

Responsible entities use various methods or processes for determining active vendor remote access sessions. It is important to note that while not required, a method to analyze all active remote access sessions, regardless of whether they originate from a vendor, meets the intent of this requirement. Vendor remote access sessions must be included in the method to ensure a Responsible Entity has the ability to disable active remote access sessions as prescribed in requirement part 2.5. The method does not need to be able to distinguish between vendor remote access sessions and non-vendor remote access sessions.

Implementation Guidance for Vendor Interactive Remote Access

Below are some examples of approaches to comply with this requirement for Interactive Remote Access:

- A Responsible Entity controls Interactive Remote Access using multi-factor authentication: One common method for determining active vendor Interactive Remote Access is for the Responsible Entity's operators or other personnel to maintain possession of part of the remote access authentication credentials, such as a token assigned to the vendor. The entity documents a procedure of how the vendor contacts

the Responsible Entity to state their need for remote access and to verbally obtain the current token code for login. The Responsible Entity can maintain a log (automated by the system or manually by an operator) which provides evidence of implementation of this method. Or, rather than hold a token, the Responsible Entity can implement a process where all vendor accounts are normally disabled until a vendor contacts the Responsible Entity by phone, validates their identity, resulting in the account being enabled for the period required.

- A Responsible Entity can document a method that uses a physical disconnect on communication circuits used for vendor remote access: Various forms of hardware devices exist where upon activation will connect a physical communications circuit for a period of time and then automatically physically disconnect the circuit after a preset time period. When deploying this method, the Responsible Entity documents how the vendor communicates with the Responsible Entity to activate the communications circuit and the logging of that event.
- A Responsible Entity can document a method whereby personnel issue commands that interrogate the systems involved (including Intermediate Systems or authentication systems) and produce a listing of currently active remote access sessions: For example, on a Microsoft Windows system, the query user command in Powershell ("quser /SERVER:<servername>") will display information about all users logged onto the system. Since all Interactive Remote Access sessions must use an Intermediate System, it is sufficient to have this capability on the Intermediate System. It is not necessary to demonstrate this capability on each and every BES Cyber System. Rather, the capability to collect this information in a single location is beneficial in the event of a Cyber Security Incident.
- A Responsible Entity can document its methods that use the manual connection of phone lines to modems for vendor remote access: The method would need to include how the vendor contacts the Responsible Entity to establish the need for remote access, the procedure to establish the remote access such as what phone line is connected to what modem on what system, and importantly the procedure for manually disconnecting the phone line after the remote access session is ended. A log can be kept that would document the connect and the disconnect dates and times for the phone line(s).

Implementation Guidance for Vendor System-to-System Remote Access

Methods for determining active vendor system-to-system access are generally more difficult as it involves applications establishing sessions to other applications, often at a programmatic level, across a network with no human involvement. An example would be as a control system comes up, an application on a server establishes a connection to a remote vendor historian and begins sending data for an unlimited duration. These types of connections are often used by the vendor for system health monitoring or trending purposes to know when preventative maintenance may be required on the control system itself or the asset the control system is monitoring.

Determining the active sessions for this type of vendor remote access is typically going to consist of methods for combing event logs or interrogating the systems in question to determine active sessions at the machine or system level. One additional consideration for system-to-system remote access sessions is it may be advantageous to specifically denote those that are from vendors. For the Interactive Remote Access scenario above, if an incident occurs the Responsible Entity may want to disconnect/disable all Interactive Remote Access,

but in the case of system-to-system access the entity probably cannot disable all system-to-system connectivity without large impact to BES Cyber Systems. The ability to discern which system-to-system sessions are truly vendor remote access may be much more necessary for these types of connections.

Below are some examples of approaches to comply with this requirement for system-to-system access:

- A Responsible Entity can document a method for how they comb or filter event logs on the system to look for session initiation or teardown events to determine active sessions. This could be accomplished through manual processes to review log data or through the automated correlation capabilities of a Security Information and Event Management (SIEM) system.
- A Responsible Entity can document a method whereby the commands that could be issued to the system to interrogate active sessions and determine which sessions are active system-to-system vendor remote access sessions. For example, the entity's method could include specific netstat commands that list active sessions along with instructions on the ports, programs, or destination addresses that would denote a session as a system-to-system vendor remote access session.
- A Responsible Entity can document a method that determines the active sessions at an Electronic Access Point (EAP) as the session crosses the Electronic Security Perimeter (ESP). For example, the commands the Responsible Entity could use on a firewall to list the connection table and determine which sessions are vendor remote access sessions. Alternatively, a method could involve looking at the access rules in an EAP that allow the traffic to the vendor and being able to determine from the 'hit count' that the session is active. Similar methods could also be used with a host based firewall on the BES Cyber System as well.
- A Responsible Entity can document a method that determines the active sessions using network monitoring techniques such as netflow monitoring or full packet capture of remote access sessions. The entity could use manual instructions or automated recognition to denote vendor remote access sessions based on ports, programs, or destination addresses.

Requirement Part 2.5

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

Implementation Guidance for Requirement Part 2.5

As requirement part 2.4 documents the Responsible Entity's method for determining the active vendor remote access session, this requirement part documents the Responsible Entity's method to disable those sessions. These methods can be documented separately or together with the methods in 2.4.

Implementation Guidance for Vendor Interactive Remote Access

Below are some example approaches to comply with this requirement for disabling vendor Interactive Remote Access:

- Methods to disable the vendor user account such that it will not successfully authenticate to the entity's system until reenabled.
- Notification methods to operators or other personnel to not disclose token codes or other authentication factors if called by vendors.
- Methods to disable Intermediate Systems such that no remote access is allowed. Examples of this approach include disabling accounts on the Intermediate System, shutting down the Intermediate System, disconnecting the Intermediate System from the network (logically or physically), or modifying EAP access lists to block access to the Intermediate System.
- Methods to disable active vendor access at the Intermediate System or the BES Cyber System itself. On a Microsoft Windows system, a session can be terminated using the Powershell logoff command ("logoff [sessionname | session ID] /SERVER:<servername>").
- Methods to physically disconnect cables or circuits to disable active vendor access.

Implementation Guidance for Vendor System-to-System Remote Access

Below are some example approaches to comply with this requirement for disabling system-to-system vendor remote access sessions:

- Documentation of commands used to terminate processes that initiate or accept sessions to or from remote vendor systems and prevent their execution.
- Methods to disable or modify access rules in EAPs such that the traffic may not leave or enter the ESP to or from the vendor's system(s).
- Methods to physically disconnect cables or circuits over which vendor connectivity occurs, or to activate physical disconnect switches.
- Methods that aggregate all vendor remote access on a separate VPN appliance or security gateway such that that device can be disabled or shut down, effectively terminating all vendor remote access.

Appendix A: Vendor Remote Access Reference Model