NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions

November 25, 2014
CIP Version 5 Standards

This document provides answers to questions asked by entities as they transition to the CIP Version 5 Standards. The questions are listed by the CIP Version 5 standard requirement for which they are associated, and will be updated periodically throughout the Transition Period as new questions arise. The information provided herein is intended to provide guidance to industry during the CIP Version 5 transition period and is not intended to establish new requirements under NERC's reliability standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time.

CIP Version 5 Standard	Question	Answer
CIP-007-5, R3, Part 3.2 Mitigate the threat of detected malicious code.	For the implementation of malicious code prevention, should entities choose to deter, detect, or prevent malicious code? If an entity chooses to deter, how should they plan on complying with CIP-007-5, R3, Part 3.2 since there would be no mechanism to detect? Is there an implicit requirement in Part 3.2 to deploy detective controls?	Part 3.2, in and of itself, does not have an implicit requirement to deploy detective controls; rather, Part 3.2 works in concert with other CIP requirements, such as CIP-007-5, R4, Part 4.1.3 which requires logging for malicious code. Under Part 3.2, Responsible Entities have an obligation to mitigate malicious code whenever it is detected through any means. Responsible Entities have asked what the relationship is between Part 3.1 and Part 3.2. Whereas Part 3.1 gives Responsible Entities the choice of deploying deterrence, detective, or preventive controls, Part 3.2 simply states detected malicious code must be mitigated.
CIP-010-1, R1, Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production	If the vendor of a system tests and verifies that patches are compatible with their system, up to and including all support components of the system, does that vendor testing meet the requirements of	The answer depends on how closely the vendor has simulated the entity's environment. Does the vendor take into account all of the customizations the entity has built-in to their solution? Does the

CIP Version 5 Standard	Question	Answer
environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	CIP-010-1 or will further testing at the facility be necessary before the patch is installed?	vendor's hardware match the entity's hardware? The vendor's testing has to be representative of the entity's production environment and where deviations exist they must be documented and accounted for with counter measures. Any entity not running the current release version, whether or not customized, cannot rely upon the vendor unless the vendor can demonstrate that the Responsible Entity's software version, including any customizations, was tested at the factory. Additionally, vendor testing should be focused on addressing CIP Standards requirements for testing and not simply on functional testing; maintenance contracts with the vendor should specify what the vendor is testing and the vendor needs to provide documentation of the testing to the customer in order to demonstrate compliance.
CIP-002-5, R1 Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 3:	Some of the systems not previously covered under the CIP Standards before may fall under the assessment process under CIP V5. Do we assess the systems that could cause the EMS (BES Cyber Assets) to fail such as UPS, HVAC (building power control system and cooling for computer room)?	HVAC, UPS, and other support systems are not the focus of the CIP Standards and are outside the scope of the CIP Standards, unless any such support systems, including HVAC and UPS, are within an ESP. If such support systems are within an ESP, these systems would be a PCA inheriting the highest impact rating within the ESP.

Comments Received – FAQ Posted November 25, 2014	
Organization	**Comment**
General Comments	
Edison Electric Institute	We continue to support NERC's process for developing supporting documents to aid stakeholders in the implementation and understanding of the CIP Version 5 Cyber Security Standards. To ensure that these supporting references will receive an open and inclusive technical review, we make the following process recommendations: 1. Establish a clear and consistent mechanism to notify stakeholders of the FAQ and Lessons Learned postings (e.g., use one email list and make it known on the NERC Transition website: http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx, 2. Clearly identify the due dates, in addition to the posted dates in each FAQ and Lesson Learned document as well as the NERC Transition website, and 3. Allow a 30-day public comment period to provide stakeholders adequate time to carefully review and comment on the documents.
Specific Comments	
Simon Cyber Group	CIP-007-5 Requirement R3 requires the prevention of malicious code. [FERC Order 791, par. 128] Prevention cannot be effectively achieved without the deployment of detective controls. The suggested answer is inconsistent with the stated rationale for CIP-007-5 R3, which emphasizes that the purpose of the requirement is to both limit and detect malicious code from adversely affecting the Cyber Assets of a BES Cyber System. "Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System." An alternative answer to the question concerning the interpretation of R3.2 is as follows: There is an implicit requirement in Part 3.2 to deploy detective controls. The rationale for CIP-007-5 R3 emphasizes that the purpose of the requirement is to both limit and detect malicious code from adversely affecting the Cyber Assets of a BES Cyber System. The express language used in Part 3.2, which refers to the mitigation of "detected malicious code," inherently requires the deployment of detective controls. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. While Part 3.2 does not prescribe or require a single method for protecting against the introduction of viruses or malicious software to a cyber asset, there must be one or more methods that collectively limit and detect malicious code.

Comments Received – FAQ Posted November 25, 2014	
Organization	**Comment**
Edison Electric Company Wisconsin Electric Power Company Exelon	We support the direction taken in the answers to the three FAQs posted on November 20. However, the answer for the question related to CIP-010-1 R1, Part 1.5 contains language that is not supported by the language of the standard, specifically the last two sentences of the answer: "Any entity not running the current release version, whether or not customized, cannot rely upon the vendor unless the vendor can demonstrate that the Responsible Entity's software version, including any customizations, was tested at the factory. Additionally, vendor testing should be focused on addressing CIP Standards requirements for testing and not simply on functional testing; maintenance contracts with the vendor should specify what the vendor is testing and the vendor needs to provide documentation of the testing the customer in order to demonstrate compliance." The first sentence above that starts with "any entity" is not supported by the language of CIP-010-1 R1, Part 1.5 and conflicts with the Guidelines and Technical Basis for this standard. The standard states that the test must be performed in a manner that "models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected." It also requires documentation of the "differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environment." This language gives the Responsible Entity flexibility to determine how to best model the test environment, accounting for differences from the production environment, and does not require entities to mirror release versions and customizations. The Guidelines and Technical Basis for CIP-010-1 also states on page 38 under the test environment section that: "the requirement is to 'model' the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to replicated or duplicated exactly." This guidance also conflicts with the FAQ sentence that requires the version to be replicated exactly. Because this sentence in the answer to the FAQ is not supported by the language of the standard and conflicts with the guidance, we recommend removing it from the FAQ. The next sentence that starts with "additionally, vendor testing" also inappropriately adds a contracting requirement "maintenance contracts with the vendors should specify what the vendor is testing and the vendor needs to provide documentation of the testing the customer in order to demonstrate compliance." Although this might be a good idea, if feasible (e.g., if a maintenance contract is used and the vendor agrees to the terms), it is not required by CIP-010-1, R1, Part 1.5. How the Responsible Entity meets the requirement is not described or

Comments Received – FAQ Posted November 25, 2014	
Organization	**Comment**
	mandated by the standard. Therefore this sentence should also be removed from the answer as it is not supported by the language of the standard. In this FAQ, the question simply asks whether vendor testing can meet the requirements of CIP-010-1 and the answer is clearly given in in the first four sentences, which essentially states that it depends on whether the vendor's testing is representative of the production environment, allowing for deviations if they are accounted for with counter measures.
Duke Energy Corporation	• CIP-007-5 R3, Part 3.2 – No comments • CIP-010-1 R1, Part 1.5 – The first sentence of the third paragraph, "Any entity not running the current release version, whether or not customized, cannot rely upon the vendor unless the vendor can demonstrate that the Responsible Entity's software version, including any customizations, was tested at the factory" is unsupported by the CIP Standard and in conflict with the Guidelines and Technical Basis of CIP-010 that was released with the Standard by the SDT. o The Standard simply says that the test environment must "model the baseline configuration" but makes no specific reference to mirror release versions and customizations. The words in the Standard provide the necessary flexibility to the entity to determine how best to model the environment without creating specific elements of the baseline as suggested by the FAQ must be identical. o The Guidelines and Technical Basis for CIP-010-1 provides guidance on the test environment on Page 3 in the Test Environment section and states "the requirement is to 'model' the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to replicated or duplicated exactly.". This Guidance is in direct conflict with the FAQ language that prescribes elements of a baseline that have to be duplicated exactly. o Based on conflicting language in the Guidelines and Technical Basis and the flexibility of the Standard I recommend removing this sentence from the FAQ. • CIP-002-5, R1 – The entire response is not supported by the CIP Standard and NERC-Approved definitions. The response states that these systems are "outside the scope of the CIP Standards, unless any…are within an ESP". o CIP-002-5's Exemption section (4.2.3) lists a few examples of Cyber Assets that are exempt from following CIP-002-5. As these systems (UPS, HVAC, etc.) are not listed, the entity's must comply to these devices if they become applicable within the language of CIP-002-5. o By definition, a BES Cyber Asset is "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems,

Comments Received – FAQ Posted November 25, 2014	
Organization	**Comment**
	or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System". The definition doesn't provide any exemptions for particular Cyber Assets as suggested by the FAQ response. This leaves ambiguity if an entity finds it has a Cyber Asset that is associated with a UPS or HVAC system that meets the definition of a BES Cyber Asset but is being directed by this FAQ that it is outside of the scope of CIP. o The response additionally leaves ambiguity as to whether or not other Cyber Assets that meet the definition of a BES Cyber Asset can also be considered "outside of the scope of the CIP Standards". o Based on the conflicting language within the Standard and NERC-approved definitions I recommend deleting the current answer and leveraging the definitions to support the possibility that Cyber Assets that support UPS, HVAC systems could now be considered within CIP scope if they meet the definition of a BES Cyber Asset or are otherwise located within an ESP.