NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions

CIP Version 5 Standards

Consolidated FAQs and Answers

Version: October 2015

This document is designed to provide answers to questions asked by entities as they transition to the CIP 5 Reliability Standards. 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.

This document consolidates several sets of FAQs that had been posted for stakeholder comment, reviewed and revised as appropriate, and approved by the Standards Committee as follows:

- FAQs posted for stakeholder comment on November 25, 2014
- FAQs posted for stakeholder comment on April 1, 2015
- FAQs posted for stakeholder comment on May 1, 2015

Note: The "number" column in the table below is not relevant to stakeholders and is only included as an organizational tool for NERC.

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-002-5.1 Requirement R1 Attachment 1	How is 1500 MW determined under CIP-002-5.1, Attachment 1, criterion 2.1?	It is the net Real Power capability, which is the gross Real Power capability less any auxiliaries, station service, or other internal use of the output of	45

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		generation units. The following are examples that could be used for determination of Net Real Power: • Any method approved by a Transmission Planner or Reliability Coordinator • Industry accepted engineering studies of net generation output, such as may be required of market participants. • The highest aggregate net generation output (e.g., from an entity's energy accounting software, NERC standard MOD-024-1, MOD-025-2).	
CIP-002-5.1 Requirement R1 Attachment 1	What is a "shared" BES Cyber System?	Shared BES Cyber Systems are those that are associated with any combination of units in a single interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criteria 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single interconnection." For criteria 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-02-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems for further information and examples.	49

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-002-5.1 Requirement R1 Attachment 1	How can we show that there is not a 15 minute impact on BES (what evidence needs to be supplied)?	CIP-002-5.1, R1 requires Responsible Entities to consider a listed set of assets and identify each of the high, medium, or low impact BES Cyber Systems using Attachment 1. The standard does not require entities to identify Cyber Assets (or provide evidence on Cyber Assets) that are not BES Cyber Systems. The measure for R1, M1, provides examples of acceptable evidence to meet the R1 identification of high and medium impact BES Cyber Systems, including dated electronic or physical lists of the high and medium impact BES Cyber Systems."	52
CIP-002-5.1 Requirement R1 Attachment 1	Should entities who receive an XML feed from [their ISO/RTO] as a backup to their ICCP (BES Cyber Asset) consider that as an in-scope resource for CIP Version 5? Is that part of a Medium Impact BES Cyber System?	Redundancy is not an exclusionary consideration in identifying BES Cyber Assets and by extension BES Cyber Systems. If the Cyber Asset, including Cyber Assets that receive backup XML feeds, has an impact on the BES, consistent with the definition of a BES Cyber Asset, then it must be classified and protected as a BES Cyber Asset regardless of other Cyber Assets that perform the same function as this Cyber Asset. Each system should be considered separately for its impact on the BES, including backup/redundant systems.	58
CIP-002-5.1 Requirement R1 Attachment 1	Where do tie line meters with dial-up modems fall under CIP V5?	Applicability under CIP V5 depends on the characteristics of the assets (Transmission substations) where the metering equipment is installed and the operating voltage of the tie line the meter is reporting.	77

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		If the data reported by the metering system is used for real-time situational awareness, the Cyber Assets associated with the metering will likely be either medium or low impact BES Cyber Assets or BES Cyber Systems, based upon the application of Impact Rating Criteria 2.4, 2.5, 3.2, and potentially 2.6 and 2.8. Once categorized as medium or low impact, the applicable CIP Standards requirements are determined by the applicability statements in each requirement. Certain requirements will be applicable regardless of how the metering BES Cyber Systems communicate with the Control Center. If the BES Cyber Asset is connected to a routable network, even if the routable network is local only to the substation, an Electronic Security Perimeter and Electronic Access Point is required. If the metering BES Cyber Systems are connected serially, the BES Cyber Systems are not required to reside within an ESP. If the metering BES Cyber Systems are dial-up accessible, authentication of the dial-up connection is required where technically feasible.	
CIP-002-5.1 Requirement R1 Attachment 1	If the same PACS system is used for both high and medium locations, do the protections need to be provided at the high level for all locations?	The definition of the Physical Access Control Systems (PACS) is "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." PACS are also associated with providing protections of BES Cyber	89

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		Systems. If the same PACS system is used to control physical access to both high and medium impact BES Cyber Systems, then all of the requirements for high and medium impact BCS that include their associated PACS would apply to that single PACS system regardless of the facility at which the PACS may reside. However, requirements for high and medium impact BCS where PACS is not listed as an associated Applicable System would not apply to that single PACS system.	
CIP-002-5.1 Requirement R1	When identifying BES Cyber Assets, how should entities approach the term "misuse"? If one Cyber Asset can be misused which impacts another Cyber Asset which then impacts the BES, do all the Cyber Assets need to be considered BES Cyber Assets?	The term "misuse" means that the Cyber Asset is being used for a purpose other than its designed use. If misuse of the Cyber Asset would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System, then the Cyber Asset should be classified as a BES Cyber Asset. Referring to the question, each Cyber Asset should be considered individually for inclusion as a BES Cyber Asset based on the definition of a BES Cyber Asset. If a Cyber Asset is determined to not be a BES Cyber Asset, the Cyber Asset should be analyzed to determine if any other classification (i.e., EACMS, PACS, or PCA) is warranted.	36

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-002-5.1 Requirement R1 Attachment 1	What should be considered when determining whether a Transmission Scheduling System is a BES Cyber System, and if so, is it a medium or high impact BES Cyber System?	A Transmission Scheduling System may contain BES Cyber Assets depending on its functionality and how it is used by the Responsible Entity to support the reliable operation of the BES. In order to determine if the Transmission Scheduling System is composed of BES Cyber Assets, assume the data associated with the system is rendered unavailable, degraded, or misused, and if this would adversely impact the reliability of the BES within 15 minutes. If the Transmission Scheduling System is determined to be a BES Cyber System, its impact rating will be determined by the Control Center or other Facility where the Transmission Scheduling System is located as provided in Reliability Standard CIP-002-5.1 Requirement and Attachment 1.	53
CIP-002-5.1 Requirement R1 Attachment 1	In Attachment 1 of CIP-002-5.1, impact rating criterion 1.4 states “Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criteria 2.1, 2.3, 2.6, or 2.9.” The phrase “one or more of the assets for criterion 2.1 …” is unclear as the criterion 2.1 identifies “groups” of generators. Are the “assets” in criterion 1.4 the “groups” in 2.1 or the generators within the groups?	Impact rating criterion 2.1 references groups of generating units at a single plant location. For these impact rating criteria, each individual generating unit is not considered an asset. The asset described in impact rating criterion 2.1 is the commissioned generation with an aggregated net Real Power capability of 1500 MWs at a single plant location. The group of generating units could range from one unit to many units, but it is the single plant location that	61

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		defines the applicable asset in the case of impact rating criterion 1.4.	
CIP-002-5.1 Requirement R1	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)?	If a device meets the definition of a Cyber Asset, as defined in the NERC Glossary of Terms, then it is subject to consideration as a BES Cyber Asset as defined in the NERC Glossary of Terms. HVAC, UPS, and other support systems are not the focus of the CIP Standards and will not be the focus of compliance monitoring, 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.	3-2014
CIP-003-6 Requirement R2	Is RFC 1490 Protocol considered serial? Routable?	RFC 1490 is an encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. If IP traffic is encapsulated in this protocol (if the traffic leaves the ESP as routable and is routable at the destination network), then it would be considered to be a routable protocol.	22

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-003-6 Requirement R2	Is IEC 61850 a routable protocol (for purposes of high and medium impact)?	IEC 61850 is an Ethernet-based standard for the design of electrical substation automation and the abstract data models can be mapped to a number of protocols, including MMS (Manufacturing Message Specification, the underlying communication architecture for ICCP), GOOSE, and Web Services. IEC 61850 is not a data link or network layer protocol, thus declaring IEC 61850 to be a routable or non-routable protocol is not appropriate. Time-critical messages, such as GOOSE messages for direct inter-bay communication, typically run on a flat Layer 2 network without the need for Layer 3 IP addresses. Other non-time-critical messages, including MMS and web services, typically run on a Layer 3 network, such as TCP/IP, with addressing and routing. The registered entity should carefully evaluate the communication environment supporting the IEC 61850 data protocol to determine if routable communication exists. If the IEC 61850 data is being communicated over a TCP/IP network, then that network connectivity is considered routable and should be protected per the CIP Standards accordingly. Note: Low impact requirements exempt 61850 from its scope as stated in the Guidelines and Technical Basis for CIP-003-6 R2: “The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g.,	23

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, specifically exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," such as IEC 61850 messaging."	
CIP-004-6 Requirement 4 Part 4.1	In the event of a CIP Exceptional Circumstance, does an entity have to meet all of the CIP requirements that do not specifically mention CIP Exceptional Circumstance?	Yes, unless specifically called out in the requirement part with the phrase "except during CIP Exceptional Circumstances", compliance to the CIP version 5 standards and requirements must be maintained. Note that CIP-004-6 R4 Part 4.1 includes CIP Exceptional Circumstances for authorizing electronic access, unescorted physical access and access to designated storage locations for BES Cyber System Information. Consequently, an entity may consider specific procedures surrounding a CIP Exceptional Circumstance in its CIP-011-2 R1 Part 1.2 procedure for protecting and securely handling BES Cyber System information, including storage, transit and use. Access to BES Cyber System Information may be controlled in accordance with the requirements of CIP-004-6, which provides for a CIP Exceptional Circumstance, that CIP-011-2 does not allow.	62

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		Consider also, for example, that the measures column for CIP-004-6 R2 Part 2.2 includes the phrase, "documentation of when CIP Exceptional Circumstances were invoked."	
CIP-004-6	Does the CIP-004-6 standard require separate training for each role, function, or responsibility? "	No, the CIP-004-6 standard does not require separate straining for each role, function, or responsibility. All nine elements have to be addressed collectively across all the training but the entity has flexibility to determine which content areas are appropriate for each role. Refer to the Guidelines and Technical Basis in CIP-004-6 for more information.	63
CIP-004-6	For access revocations due to a termination, reassignment, or transfer, when does the clock start for revocation obligations and when must revocation be complete?	From the CIP-004-6 Guidelines and Technical Basis states "the timing of the termination action may vary depending on the circumstance" and goes on to specify possible processes associated with termination scenarios. For terminations, the 24-hour clock starts when the entity takes action to terminate according to their process. As an example, the action to terminate could be the notification to the individual of their termination, and then removal of unescorted physical access and Interactive Remote Access must complete within 24 hours after notification.	64

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		For reassignments or transfers, the entity must establish a date when the individual no longer needs access. Revocation must then occur by the end of the next calendar day after this entity established date. Business days are not taken into consideration for this requirement. Entities should be careful to observe these timeframes even on weekends and holidays.	
CIP-005-5 Requirement R1	If Part 1.4 (Dial Up Connectivity) applies, what other requirements apply to that system and their associated PCA?	Refer to the "Applicable Systems" column for each requirement to determine what other requirements apply. For example, if the system is a medium impact BES Cyber System (not at a Control Center and without External Routable Connectivity), many other requirements apply. Applicable requirements are identified by referring to the "Applicable Systems" column for "medium impact BES Cyber Systems." Dial-up connectivity is a specific connection mechanism applied to High and Medium Impact BES Cyber Systems under CIP-005-5 R1 Part 1.4. All other CIP V5 standards applicable to High and Medium Impact BES Cyber Systems would apply, depending on impact classification of the specific BES Cyber System and a lack of unique criteria on the "Applicable Systems" column to specifically exclude the BES Cyber System.	80

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-005-5 Requirement R1	If a Responsible Entity implements a vendor appliance as the perimeter firewall, can the optional module to perform the monitoring function reside on the same appliance?	Yes, the module can reside on the same appliance. Reliability Standard CIP-005-5 Requirement R1.5 requires "one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications". This requirement does not specify that two or more physical devices be used to monitor inbound and outbound communications. Ref. the Guidelines and Technical Basis in CIP-005-5 for additional information.	76
CIP-005-5 Requirement R2	When a desktop/laptop is used to log in to a jump box (Intermediate System) should the desktop/laptop have the same physical controls as the assets it is accessing?	In this example, the desktop/laptop is not part of a BES Cyber System, as it is outside of the ESP and uses appropriate measures for Interactive Remote Access. The jump box (Intermediate System) would be considered an EACMS and must meet the requirements that apply to an EACMS. It would not be necessary for the desktop/laptop to also meet the requirements.	73
CIP-005-5 Requirement R1	Can there be Protected Cyber Assets (PCAs) associated with medium impact BES Cyber Systems at transmission substations where there is no External Routable Connectivity?	Reliability Standard CIP-005-5, R1 Part 1.1 requires that medium impact BES Cyber System(s) that are connected to a network via a routable protocol, even if they have no external routable connectivity, must reside within a defined ESP. A PCA is any Cyber Asset that resides on the routable network contained within the ESP, but is not otherwise classified as a BES Cyber Asset or EACMS. This designation of PCA is without consideration of External Routable Connectivity. There are several requirements in the reliability standards that are	21

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		applicable to "medium impact BES Cyber Systems and their associated PCA".	
CIP-005-5 Requirement R1	Regarding CIP-005-5, page 16 in the Guidelines for R1, what is required of the ESP defined for a standalone network (Medium Impact BCS at a substation that meets CIP-002-5.1 Requirement R1, Attachment 1, Criterion 2.5 that has no External Routable Protocol)?	As required under CIP-005-5, R1, Part 1.1, "all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP." Each of the CIP V5 requirements must be reviewed by the Entity to determine their applicability to a medium impact BES Cyber System. Some of the requirements further qualify the "applicable systems," and others do not, making them applicable to those medium impact BES Cyber Systems without External Routable Protocol. If there is dial-up connectivity to the medium impact BCS, then CIP-005-5, R1, Part 1.4 applies as well. If it's truly standalone (no ERC), then the Entity should document the perimeter to prove the components of the BCS are within the ESP.	81

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-006-6 Requirement R1	For a substation with Medium Impact BES Cyber Systems, can the ESP be extended to include two control houses with buried cable between the two? Will this communication require alarms, encryption, or something else to meet the draft CIP-006-6 requirements for the revisions to CIP-006-6?	Entities can determine how they want to define their ESPs. For the CIP-006-6 R1 Part 1.10 revisions, entities are required to physically protect cabling that extends outside the Physical Security Perimeter for high impact and medium impact Control Centers. Burying the cables or running continuous conduit can be an approach to restricting physical access. Additionally, applying encryption over the connection is also an approach that can be used. CIP-006-6 R1 Part 1.10 revisions do not apply to substations.	83
CIP-006-6 Requirement R1	What are the options for utilizing two or more different physical access controls for High Impact BES Cyber System Physical Security Perimeters?	The Guidelines and Technical Basis for CIP-006-6, R1 states: "The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are)..."	86

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-006-6 Requirement R3	What does the testing requirement in CIP-006-6, R3, Part 3.1 mean for PACS workstations and servers? Does that need to be documented the same way the card readers/door alarms are?	PACS workstations and servers should be tested in such a way to demonstrate "they function properly" as required in Part 3.1. Since these Cyber Assets do not perform the same functions as the card readers/door alarms, the actual testing and documentation may differ. Sufficient evidence should be documented to demonstrate the Cyber Assets were tested and "function properly". Functional tests may include, but are not limited to, granting, revoking, monitoring, and logging of access. One method of accomplishing this would be to: (a) create a set of test scripts for the Cyber Assets (collectively or individually) to demonstrate they are functioning properly, (b) execute them as required, (c) and document the results of the executed tests. Verification of the PACS functioning under normal operations would also suffice.	90
CIP-006-6 Requirement R1	Is CIP-006-6 R1 Parts 1.6 and R1.7 intended to including monitoring and alerting on guard and badging workstations?	Yes, CIP-006-6 R1 Parts 1.6 and 1.7 are intended to monitor and alert on potential unauthorized physical access to the PACS systems. In accordance with CIP-006-6, R1, Part 1.6, devices that make up the PACS system including servers, controllers, and workstations should be brought into scope for this requirement. Depending on the configuration, some guard and badging workstations may not be PACS associated with high or medium impact BES Cyber Systems and,	91

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		therefore, monitoring and alerting would not be required for the workstations not considered PACS.	
CIP-007-6 Requirement R5	What are examples entities may use when inventorying all known enabled default or generic account types?	Some of the ways to identify default and/or generic accounts include: • Vendor provided lists of the required accounts on a system. • Tools that can be run to identify user accounts created on a local system. • Tools such as AD (or LDAP Queries) may have a listing of accounts with access to systems. • Review the device/application web sites or support to identify if there are default accounts.	92
CIP-007-6 Requirement R5	Are password safes recommended?	A password safe is a utility application that is used to securely store a set of passwords and pass phrases. While the ERO Enterprise (NERC and the Regional Entities) cannot recommend or endorse the use of any particular technology, password safes can be an effective tool in an organization's overall cybersecurity program when used properly, and their use, providing any information contained within the password safe meets the definition of BES Cyber System Information, should adhere to the entity's CIP-011-2 Information Protection program. In addition as a best practice, the password safe's passphrase should require periodic change and meet defined password criteria. For example, an entity may consider CIP-007-6, Parts 5.5	93

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		and 5.6, and if shared with multiple individuals, CIP-007-6, Part 5.3.	
CIP-007-6 Requirement R1	Signage for physical port protection (CIP-007-6, R1.2) – is it acceptable to place signs at the PSP doors, rather than on each individual device port?	Signage is explicitly allowed as a measure of compliance. If a sign is used, then its placement and the language used on the sign are both considerations for determining whether it conveys that the port should not be used without proper authorization. The Guidelines and Technical Basis for CIP-007-6 R1 states "In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders…". In addition, the requirement does not require demonstrating that a protected, physical input/output port that is unnecessary for network connectivity, console commands, or removable media has not been used. For more details, refer to the measures column, the guidelines and technical basis, and violation severity level in the standard for this requirement. For example, the guidelines and technical basis for the requirement states: "this control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders…signage would be used to remind authorized users to "think before you plug anything into one of these systems which is the intent.	94

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		Note that this FAQ replaces the draft lesson learned "CIP-007-6 R1 Part 1.2: Protecting Physical Ports: Tamper Tape, May 27, 2014".	
CIP-007-6 Requirement R5	How should an entity treat the devices that do not have accounts but use separate passwords to delineate the role of the user? (substations). What about situations where there are no accounts, only passwords, but the users don't have access to the passwords?	Include devices that utilize passwords without an associated user ID in the CIP-007-6 R5 Part 5.2 inventory of known enabled default or other generic account types. In these cases, a null account name may be used. It may be advisable to include a field in the inventory where additional identifying details can be associated with the null account name, such as a brief description of the user role associated with that password. For those BES Cyber Assets identified as being accessible by such a password, access to a Cyber Asset with only a password should be considered a "generic account type," and individuals who have authorized access to these shared type of accounts should be documented as such. Entities are not expected to document the passwords themselves for these "generic account types." Caution: Evaluate if these are default passwords.	101

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-007-6 Requirement R3	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-007-6, 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-007-6, 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.	1-2014
CIP-007-6 Requirement R3	For CIP-007-6 R3 Part 3.1 on malicious code, is hardening or group policy sufficient?	“System hardening" and "policies," etc. have been provided as examples of acceptable measures of meeting the requirement to "deploy method(s) to deter, detect, or prevent malicious code". These methods are defined as acceptable, they should be documented in such a way to demonstrate their applicability to the desired BES Cyber Systems and their ability to provide the required control. Refer to the Guidelines and Technical Basis of CIP-007-6 R3 that includes: “Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to	98

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc."	
CIP-010-2 Requirement R1	Question 1: What level of testing should be done to develop baselines? Question 2: Are entities expected to perform a penetration test for CIP-010-2? If so, what is the appropriate scope?	Response 1: Testing (e.g., penetration testing) is not specifically required to develop a baseline, but all five parts of CIP-010-2, R1, Part 1.1 must be a part of the baseline. In some cases automated tools may be necessary to develop the baseline, for example logical ports identification as a part of the baseline and in accordance with CIP-007-6, R1, Part 1.1. Response 2: Penetration testing is not required for CIP-010-2 (but could be utilized at the discretion of the entity), but an active vulnerability assessment is an option under CIP-010-2, R3, Part 3.1, and a requirement under CIP-010-2, R3, Part 3.2. An active vulnerability	107

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		assessment is described in the Guidelines and Technical Basis section of CIP-010-2, R3.	
CIP-010-2 Requirement R3	How should active vulnerability scans be managed for environments sensitive to denial of service impacts?	CIP-010-2, R3.1 gives responsible entities the option to conduct a paper or active vulnerability assessment. Accordingly, the responsible entity should choose the option that will yield the optimal results given the potential susceptibility to denial of service attacks. For instances, if the environment is highly susceptible to denial of service attacks, then the entity should only conduct paper vulnerability assessments or avoid the use of denial of service vulnerability testing. It is important to note that an active vulnerability assessment is required every three years for a high impact BES Cyber System and prior to adding new high impact BES Cyber Assets, EACMS or PCAs. The active vulnerability assessment requirement does not apply to PACS.	108
CIP-010-2 Requirement R3	Are Responsible Entities required to demonstrate that they have remediated against known Industrial Control Systems (ICS) vulnerabilities? What are acceptable methods to demonstrate compliance?	While it may be considered a best practice to monitor for known ICS vulnerabilities as part of an overall security program, it is not required by the CIP v5 standards. Responsible Entities are required to demonstrate that they comply with Reliability Standards CIP-007-6 Requirement R2, Part 2.1 for patch management and CIP-010-2 Requirement R3, Part 3.1 for cyber vulnerability assessments.	68

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		During an audit, the Responsible Entity may be asked to demonstrate that the required security patch assessments and vulnerability assessments have been performed and that mitigation or remediation plans have been documented and implemented as required.	
CIP-010-2 Requirement R3	What methods should Responsible Entities use to demonstrate they have performed penetration or red team tests? Are there specific tools or procedures that can be referenced?	Reliability Standard CIP-010-2 requires Responsible Entitles to perform an active vulnerability assessment at least once every 36 months for high impact BES Cyber Systems, where technically feasible. While penetration testing and red team tests are both tools an entity may choose to use in support of their vulnerability testing program, they are not required by CIP-010-2, R3, Part 3.2. As discussed in the Guidelines and Technical Basis section of CIP-010-2, less invasive testing may be performed, including active network discovery and the use of vulnerability scanning tools. See NIST 800-115 for additional guidance. Regardless of the approach used, document the design and conduct of the assessment as described in CIP-010-2 R3, Part 3.2.1, the tools used, and the results of the assessment as described in CIP-010-2 R3, Part 3.2.2.	111

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-010-2 Requirement R3	When completing a vulnerability assessment of serial devices as required of medium BES Cyber Systems, can a Responsible Entity test a representative sample of identically configured populations and demonstrate compliance based on the results, rather than test the full population? Do paper assessments require a review of the actual configuration of the BES Cyber Asset?	The standard does not provide for sample testing; however, the assessments under CIP-010-2 R3, Part 3.1 applies to High and Medium Impact BES Cyber Systems, EACMS, PACS and PCAs, and not at the device or BES Cyber Asset level. Therefore BES Cyber Assets can be grouped into BES Cyber Systems and assessed at the system level. Testing a single BES Cyber Asset and validating that other BES Cyber Assets are identically configured to the tested BES Cyber Asset is one method of dealing with large numbers of BES Cyber Assets in substation and generation environments. To demonstrate compliance with CIP-010-2 R3, Part 3.1 using a paper vulnerability assessment, Responsible Entities must document the date of the assessment, the controls assessed for each BES Cyber System, and the method of the assessment. Elements of a paper vulnerability assessment are further described in the Guidelines and Technical Basis for CIP-010-2.	112
CIP-010-2	Do the Reliability Standards require high impact Control Centers to have quality assurance environments for testing patches before implementing in the production environment? Is it acceptable for Responsible Entities to have tests performed by third parties on systems that are not exact replicas of the Entity's operational system?	Reliability Standard CIP-010-2 requires, for high impact BES Cyber Systems, Responsible Entities to "prior to implementing any change in the production 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, and models the baseline configuration to ensure that required cyber security controls in CIP-005-5 and CIP-007-6 are not adversely affected."	113

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		Responsible Entities may choose how they test patches to ensure the cyber security controls required by CIP-005-5 and CIP-007-6 are not adversely affected. CIP-010-2 R1 does not prohibit the use of third party testing, but requires that the third party system 'models' the Responsible Entity's baseline configuration. The third party system may have a different set of components than the Responsible Entity's system. The Responsible Entity should document the differences between the test environment and the production environment.	
CIP-010-2 Requirement R1	How have the requirements for testing changed from CIP-007-3a R1 to Version 5?	The changes for testing are reflected in CIP-010-2 R1 Part 1.4 and Part 1.5 and are more detailed and specific than in CIP Version 3. Both requirement parts require testing for "each change that deviates from the existing baseline configuration" in Part 1.1. Both requirement parts require determining which "required cyber security controls in CIP-005-5 and CIP-007-6" could be "impacted by the change" and verifying after a change that those controls were "not adversely affected." Additionally, CIP-010-2 R1 Part 1.5 for high impact BES Cyber Systems requires testing "the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimized adverse effects, that models the baseline configuration." For example, systems in the corporate environment that are sufficiently similar to	114

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		BES Cyber Systems in the production environment may be used for testing. If a test environment is used for Part 1.5, refer to specifics in Part 1.5.2 for required test environment documentation. Testing required under CIP-007-3a R3 for Security Patch Management was removed from CIP-007-6 as security patches are specifically identified under CIP-010-2 R1 Part 1.1.5 and thus included in the CIP-010-2 R1 Part 1.4 and 1.5 described above. Testing for CIP-007-3a R4.2, however, of antivirus and malware prevention signatures was carried forward in CIP-007-6 under R3 Part 3.3. These changes were made In response to FERC Order No. 706 directives. The standards drafting team revised CIP-007-3a R1 testing "to provide clarity on when testing must occur" and, for high impact BES Cyber Systems, also "to require additional testing to ensure that accidental consequences of planned changes are appropriately managed."	

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
CIP-010-2	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 CIP-010-2 or will further testing at the facility be necessary before the patch is installed?	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 vendor's hardware match the entity's hardware? The vendor's testing has to be representative of the entity's production environment and where differences exist they must be documented.	2-2014
CIP-011-2	For v3 Critical Assets and associated Critical Cyber Assets that will be categorized as low impact BES Cyber Systems under v5, what is expected for declassification and destruction of critical information if the facility remains in operation?	CIP-003-6 and CIP-011-2 do not require BES Cyber System Information associated with low impact BES Cyber System to be protected. When a cyber asset identified as a Critical Cyber Asset under Version 3 is categorized for the purpose of CIP Version 5 as a low impact BES Cyber System, the applicable CIP-003-6 requirements no longer apply and therefore there is no obligation to declassify or destroy the information as long as compliance with all requirements for protecting BES Cyber System information is maintained.	128
CIP-011-2	For a BES Cyber Asset in a medium impact facility, if the device breaks and has to be sent to a vendor, what does an entity need to do to ensure the integrity of the information on that device is protected as required by the standard?	CIP-011-2 does not explicitly address the case where a device must be sent to a vendor. However, in such a case when the device in question is presumably being sent to the vendor for redeployment or disposal, the responsible entity would have to comply with the requirements of CIP-011-2 R2 Part 2.1, which address the reuse of Cyber Assets. If the device is not released	129

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		for reuse or is not being disposed, the entity should either retain or wipe the BES Cyber System Information or the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2. Entities should include in their CIP-011-2 information protection program consideration of the case where a device must be returned intact to a vendor for diagnosis or troubleshooting, including how the information should be protected against unauthorized disclosure during transit and while at the vendor site. Additionally, entities should consider what actions should be taken by the vendor, and whether these actions should be included in contractual language, in the event that the device is not or cannot be returned to the entity for destruction. See FAQ #130 for media/data destruction, including if "normal" erasure methods are unavailable due to hardware failures.	
CIP-011-2	For destruction of data what would be considered a minimum standard to ensure data is destroyed? (Degausser and hydraulic crusher)	The requirement is that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. Degaussing and	130

CIP Version 5 FAQs – Consolidated FAQs and Answers			
Standard Reference	**Question**	**Answer**	**Number**
		crushing are two of many ways to destroy media. Other methods include, but are not limited to, multi-pass wiping, drilling of platters, shredding, etc. In some cases, two or more methods could be used to ensure data destruction. The Guidelines and Technical Basis offer suggestions on how the destruction can be performed, including information from NIST SP800-88.	