NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions

CIP Version 5 Standards

Consolidated Comments Received Regarding May 1, 2015 Posting

This draft document provides answers to questions asked by entities as they transition to the CIP Version 5 Reliability Standards. The information provided 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, 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. The ERO Enterprise will continue to determine compliance based on language in the NERC Reliability Standards, which may be amended in the future.

This document consolidates industry feedback on the draft answers listed below that were received by NERC on the FAQs posted for comment on May 1, 2015 and due to NERC on June 15, 2015. NERC will review all comments provided and incorporate changes before issuing a final version of the May 1, 2015 FAQs.

General Comments – May 1, 2015 Posting	
Organization	**Comment**
Wisconsin Electric	Wisconsin Electric supports the feedback comments submitted by the Edison Electric Institute on the CIP Version 5 Standards Frequently Asked Questions posted for comments on May 1, 2015.
Southern Company	Southern Company appreciates the opportunity to comment on the North American Electric Reliability Corporation's (NERC) CIP V5 Frequently Asked Questions posted on May 1, 2015. NERC has put in a substantial effort to develop this draft document and we thank NERC for these efforts. Southern Company supports the Edison Electric Institute comments on the CIP V5 Frequently Asked Questions.
CenterPoint Energy	CenterPoint Energy supports the comments Edison Electric Institute (EEI) submitted for the CIP V5 FAQs posted for comments on May 1, 2015.

General Comments – May 1, 2015 Posting	
Organization	**Comment**
EEI	We continue to support NERC's section 11 process for developing supporting documents to aid stakeholders in the implementation and understanding of the CIP Version 5 Cyber Security Standards. In support of this process, we offer the following general and specific comments. We recommend that NERC add the disclaimer used with the Lessons Learned supporting documents that make it clear that the document is not intended to establish new requirements, modify the requirements, or provide an official interpretation. The disclaimer also clearly acknowledges that "there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document" and that compliance is based on the language of the standard. The use of "must" in many of the responses is concerning in these FAQs because it implies that this supporting document is a requirement or interpretation of the standard. To address this concern, we attempted to address this in our recommended rewordings in the specific comments below. However, we did not comment on every use of "must." Therefore in general, we suggest removing "must" from all of the responses. Although the use of "should" is not as strong as "must," we recommend limiting its use as much as possible. We recommend that all of the FAQs—including those previously posted (November 25, 2014 and April 1, 2015) as well as those—be combined into one document as approved by the Standards Committee under Section 11 and organized by standard (including version) to make them easy to review by all stakeholders and update in the future. We also recommend making them available in a sortable format, e.g., Microsoft Excel. Finally, for each FAQ, include the date it was approved by the Standards Committee under Section 11. Finally, we recommend a review of each question and answer by an editor as we noticed a number of punctuation and grammatical errors throughout this document. We realize that the NERC staff may have been trying to get this out in a hurry for industry review and we did not want to comment on each error we found.
Exelon	Exelon supports the EEI comments on the third group of CIP V5 FAQs.

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

Specific Comments – May 1, 2015 Posting		
Number	**Question**	**Answer**
36	When identifying BES Cyber Systems, how should entities approach the term "misuse"? If device A is misused and impacts device B which impact devices C which then impacts the BES. Do all the devices need to be considered BES Cyber Systems?	The term "misuse" relates to intentional or unintentional actions that adversely impact the reliability of the BES. If a device is located at or associated with a facility that meets the impact rating criteria provided in Reliability Standard CIP-002-5.1 Requirement R1 and Attachment 1, then it is a BES Cyber Asset and must be protected at the appropriate impact rating. Referring to the question, each device A, B, and C needs to be considered. If a device is not a BES Cyber Asset, but is an EACMS, PACS, or PCA, it must be protected commensurate with its classification.

Organization	Comments
EEI	This question and answer is confusing and does not help to enhance stakeholder understanding and implementation of the Version 5 CIP Reliability Standards. First, the question and answer mixes the definition of BES Cyber Asset with the identification of impact ratings for BES Cyber Systems. The term "misused" is not used for identifying BES Cyber Systems. It is used to identify BES Cyber Assets. The definition of BES Cyber Assets, which includes "misused" is a part of what sets the basis for identifying BES Cyber Assets that are grouped into BES Cyber Systems. Second, the answer uses the term "device" rather than Cyber Asset and combines the high impact language "located at" with the medium impact language "associated with." Third, page 31 in the record at: http://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/C_of_C_Project2008-06_CIPv5_20120412_Final.pdf explains what misused means:

	"Commenters asked about the phrase "unavailable, degraded, or misused." These describe states of a BES Cyber Asset which could result from a Cyber Security Incident. Unavailable means that the BES Cyber Asset is unable to perform the service it is providing to the BES Facility, System, or equipment. Degraded means that it is able to provide the service, but in a degraded way (below specified capabilities). Misused means that it is being used for a purpose other than its designed use." In order to help enhance stakeholder understanding and implementation of the Version 5 CIP requirements, we recommend changing the existing question and answer to: Q: "How is the term "misused" used in identifying BES Cyber Systems?" A: "The term "misused" is not used for identifying BES Cyber Systems. It is a consideration in determining whether a Cyber Asset is a BES Cyber Asset. "Misused means that it is being used for a purpose other than its designed use." (NERC Consideration of Comments, Cybersecurity Order 706 Version 5 CIP Standards, p 31, available at: http://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/C_of_C_Project2008-06_CIPv5_20120412_Final.pdf.)"
Duke Energy	There is no basis for the definition of "misuse" in this response (either through supporting materials or dictionary definition). The second sentence incorrectly states that a device being at a location identified in Attachment 1 makes it a BES Cyber System when much more has to be considered (i.e. adverse impact within 15 minutes). Using language "needs" and "must" appears to create a requirement whereas the FAQ needs to limit itself to guidance.
SPP	Entities should have the ability to determine how misuse would impact their BES Cyber Systems and protect accordingly. Misuse is not a term with a limited number of indicators and NERC cannot possibly consider each one. Misuse must be determined by the entity based on their assets, use cases and risk appetite.
Georgia Transmission	GTC appreciates the opportunity to provide comments on these outputs from the V5 Transition study. With respect to FAQ #36, GTC is concerned that the response implies an expansion of the applicability of the FERC approved definition for BES Cyber Assets. The definition states: "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, or equipment, which, if

	destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System…". In using singular nouns "A Cyber Asset…" and pronouns "…its required…" the focus is on the impact the Cyber Asset under consideration ultimately has on the reliable operation of the BES in real time. Expansion to include designating additional devices as BES Cyber Assets which are twice removed from having an effect on the BES results in a "hall of mirrors" of inclusion. In NERC's filing to FERC in the BES Cyber Asset Survey RM13-5 dated February 3, 2015, on page 23, NERC identifies that the definition of PCA is precisely the mechanism for dealing with this "chain": "Under the CIP version 5 standards, PCAs are afforded almost the same protections as the BES Cyber Systems with which they are associated. Accordingly, while a network printer or a historian at a control center, for instance, may not perform a reliability function or meet the 15-minute parameter, entities may be required to protect those devices under the CIP version 5 standards if those devices are in an ESP. This ensures, for instance, that printers and historians on the same network as BES Cyber Systems could not be used as vehicles to perpetrate a cyber-attack against a BES Cyber System."
AEP	AEP supports the industry comments submitted by EEI.
Lincoln Electric	This provided answer does not appear to address the question being asked. A more appropriate answer might be that (in brief) the CIPs are looking to identify and protect Cyber Assets that if rendered unavailable, degraded or misused could adversely affect the BES. To the posed question; if the misuse of Cyber Asset A can adversely affect a High Impact Asset then Cyber Asset A would need to be identified as a High Impact BES Cyber System (asset). If the misuse of Cyber Asset B can only adversely affect Cyber Asset A (and not a High Impact Asset) then Cyber Asset B would not be considered a High Impact BES Cyber System. However, Cyber Asset B may still be an EACMS, PACS, or a PCA of Cyber Asset A depending on the function being performed by Cyber Asset B and whether it resides with the ESP of Cyber Asset A or not. If Cyber Asset B is a EACMS, PACS, or a PCA of a BES Cyber System it must be protected commensurate with that classification.

Security Working Group, IRC Standards Review Committee	The SWG respectfully suggests that the answer is not fully responsive to the question asked. Specifically, the question is requesting guidance regarding the cascading impact of an asset "misuse." The issue of cascading threat vectors is not contemplated in the requirement (nor should it be). Therefore, this question is moot. Each cyber asset or system must be examined on its own merit as to whether it is "…rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES." The entity's method used to identify BES Cyber Assets and Systems should determine which assets are required to perform the reliable operation of the BES and, then, examine each of those assets to determine if misused, etc., would within 15 minutes adversely impact the reliable operation of the BES. For example. If the entity uses the suggested method in the guidance section of CIP-002, they would determine which assets are required to perform each of the operations and then determine if they meet the 15 minute criteria. Taking this approach negates the need to consider cascading beyond the scope of the BES Cyber Assets or Systems.
Tri-State Generation and Transmission	Tri-State believes the statement "If a device is located at or associated with a facility that meets the impact rating criteria provided in Reliability Standard CIP-002-5.1 Requirement R1 and Attachment 1, then it is a BES Cyber Asset and must be protected at the appropriate impact rating." needs to be restated for clarity. It does not coincide with the currently published definition of BCA and CIP-002.5-1. Not all devices (meant to say Cyber Asset?) at a rated facility are BCA. Tri-State also believes that the 2nd part of the response which states "Referring to the question, each device A, B, and C needs to be considered. If a device is not a BES Cyber Asset, but is an EACMS, PACS, or PCA, it must be protected commensurate with its classification" does not answer the 2nd question. The question is not about EACMS, PACS, or PCA, it is about how many levels deep have to be considered in defining a BCA assessing the term 'misuse' from the NERC Glossary definition of BCA. Previous versions of CIP, we were told to only go one level deep. Is that a continued stance to take?
Arizona Public Service	The term "misuse" is utilized in the Standard but is not specifically defined in the NERC Glossary of Terms (as updated May 19, 2015). The first sentence of the response effectively attempts to provide a definition of "misuse"; however the response is ambiguous. An FAQ should not attempt to provide a definition where there is none in the official NERC Glossary of Terms. An appropriate level of input from industry as a whole is needed to develop a usable definition and then it should be added to the NERC Glossary of Terms per normal process.

	The question regarding transitive impact from device B or C is irrelevant if device A is a BCA. This should be clear in the FAQ response as misuse does not apply to the identification of a BCS – only a BCA.

53	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 Systems 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. Consider functions that may be part of the Transmission Scheduling System such as: • Area Control Error calculations and their use • Automatic Generation Control operation • Available Transfer Capability calculations and their use • Net Scheduled Interchange calculations and their use • Identification and monitoring of System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs) • Identification and monitoring of Flowgates • Current-day planning • Operator procedures that rely on transmission scheduling information 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.

Organization	Comments
EEI	The listing of the functions of a Transmission Scheduling System does not help clarify the answer and could instead create further confusion. We recommend deleting the bulleted list from the above answer.

Duke Energy	The section that starts with "consider functions that may be part of…" is too prescriptive and is not supported by existing guidance. The standard does not require that these functions must be considered and it is up to the entity to determine the means to assess "adverse impact to the reliability of the BES"…this response can be provided as one such option to consider.
AEP	AEP supports the industry comments submitted by EEI.
Lincoln Electric	Agree.
Security Working Group, IRC Standards Review Committee	The SWG notes that there has already been guidance issued on this topic in Lesson Learned CIP-002-5 R1: BES Impact of Transmission Schedule Systems. It is of significant concern that there would be guidance provided on a single topic in more than one reference or guidance document. The SWG recommends that, since this response clarifies and expands upon the guidance provided in the Lesson Learned, all relevant content be incorporated into the Lesson Learned and that the revised document be subjected to the applicable process for commenting, finalization, and approval. The SWG also notes that it will reserve its substantive comments on the response until all guidance on this topic has been reviewed and consolidated.
ACES	The answer provided is reusing the same content provided in the draft version of BES Impact of Transmission Scheduling Systems Lesson Learned, published on February 27th. Wouldn't this same logic apply to the entities ICCP Server and XML Receiver Backup Server? If SCADA is identified as the raw data in this explanation, then why are tools like State Estimator and Contingency Analysis missing from this list? Please remove the language regarding ATC/AFC calculations. Since ATC/AFC calculations involve selling transmission service and then is a 20 minute schedule requirement in the pro-forma tariff, these do not meet the 15-minute requirement.

61	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.

Organization	Comments
EEI	We support this question and answer.
SPP	Very clear answer. This clarity is helpful to the industry.
AEP	AEP supports this response.
Lincoln Electric	Agree.

Colorado Springs Utilities	CSU believes that the identification of facilities for the purposes of CIP-002-5.1 should be left up to the individual entity based on circumstances unique to each entity. In some cases, generation could appropriately be grouped by location, in others it is more appropriate to group by generating unit.
Arizona Public Service	Consider re-writing the question in order to assure clarity.

70	How should traffic crossing an Electronic Access Point (EAP) be monitored?	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". There are many different ways to monitor traffic crossing an EAP. If many different interfaces are used for an Electronic Access Control Monitoring System (EACMS), only the EAPs associated with BES Cyber Systems must be monitored.

Organization	Comments
EEI	We support this question and answer.
Duke Energy	Recommend removing this Q&A as no answer to the question is being provided. "There are many different ways to monitor traffic crossing an EAP". If no specifics or additional guidance are going to be provided, then the Q&A should be removed.
SPP	While it is commendable that NERC does not want to recommend a specific technical solution, providing examples of monitoring could be helpful.
AEP	This response is non-responsive to the question. The questioner is asking for acceptable practices, not whether each EAP must be monitored.

Lincoln Electric	Agree.
Security Working Group, IRC Standards Review Committee	The SWG agrees with NERC's answer. Additionally, the SWG requests that NERC consider referring the readers to the Guidelines and Technical Basis in CIP-005-5 for more information.
Arizona Public Service	This response would provide more value if it was expanded to outline example conceptual methods to identify malicious communications such as: • Identify expected communication patterns and monitor for unexpected or anomalous communications, and/or • Correlate observed communications with expected communication patterns, and/or • Implement malicious communication detection via signature-based intrusion detection systems, and/or • Etc. Alternatively, the FAQ development team could reference commonly accepted approaches for malicious communications detection, such as those outlined by NIST or other formal standards development bodies.
ACES	"There are many different ways to monitor traffic crossing an EAP." Can the Transition Team list the most common means or expected methods of monitoring traffic across an EAP?

76	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.

Organization	Comments
EEI	We support this question and answer.
Duke Energy	While arriving at an appropriate conclusion, this answer appears to interpret the requirement within the standard which should not be performed in this type of document. The document should limit itself to guidance and suggest deleting the following sentences: "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."
AEP	AEP supports this response.
Lincoln Electric	Agree.

Security Working Group, IRC Standards Review Committee	The SWG agrees with NERC answer. Additionally, the SWG requests that NERC consider referring the readers to the Guidelines and Technical Basis in CIP-005-5 for more information.	
Arizona Public Service	Although APS does appreciate the flexibility to use a single perimeter control device to perform both firewall and monitoring services; it should be noted that this response appears to be contradictory to the language in FERC Order 706, paragraph 497 which states that: "The Commission does not agree…that providing one monitored and alarmed electronic security measure provides a sufficient and balanced security measure when implemented in conjunction with required physical security measures. A single electronic device is too easy to bypass and a physical security measure cannot thwart an electronic cyber attack. Therefore, we believe it is in the public interest to require that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter."	
73	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, 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.
Organization	**Comments**	
EEI	We support this answer.	
SPP	This seems to be a similar scenario as item #36 and this answer should be applicable to it as well.	
Duke Energy	While arriving at an appropriate conclusion, this answer appears to interpret the requirement within the standard which should not be performed in this type of document. The document should limit itself to guidance.	

AEP		AEP supports this response.
Lincoln Electric		Agree.
ACES		For clarity, add “as it” after second comma in first sentence of provided answer.
68	Are Responsible Entities required to demonstrate that they have remediated against known Industrial Control Systems (ICS) vulnerabilities? What are acceptable methods to demonstrate compliance?	Responsible Entities are not required to demonstrate that they have remediated specific ICS vulnerabilities beyond complying with Reliability Standards CIP-007-5 (- Systems Security Management) and CIP-010-1 (Configuration Change Management and Vulnerability). Reliability Standard CIP-007-5, Part 2.1 requires Responsible Entities to implement a patch management process for tracking, evaluating, and installing cyber security patches for high and medium impact BES Cyber Systems and their EACMS, PACS, and PCA. Part 2.2 Security Patch Management requires Responsible Entities to assess patches identified by the entity-designated source(s) within 35 calendar days. Parts 2.3 and 2.4 require the applicable security patches to be implemented within 35 calendar days or a mitigation plan developed and implemented to mitigate the vulnerabilities of each security patch not implemented within the required 35 days. Reliability Standard CIP-010-1, Part 3.1 requires Responsible Entities to perform cyber vulnerability assessments at least once every fifteen calendar months for high and medium impact BES Cyber Systems. The vulnerability assessment may be a documentation review or an active assessment. Part 3.2, which only applies to high impact BES Cyber Systems, requires an active vulnerability assessment to be performed at least once every 36 calendar months. Similarly, a vulnerability assessment must be performed per Part 3.3 prior to adding any Cyber Asset into an Electronic Security Perimeter containing high impact BES

		Cyber Systems, again limited to Control Centers. Part 3.4 requires the results of the vulnerability assessment to be documented and an action plan developed to remediate or mitigate vulnerabilities identified in the assessment. 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.

Organization	Comments
EEI	We recommend removing the paragraphs describing CIP-007-5 Part 2.1 and CIP-010-1 Part 3.1 (they are simply repeating the requirements and do not address the question) and change the first sentence (to add the references to the standards) to: "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 responsible for compliance with Reliability Standards CIP-007-5, Part 2.1 (Systems Security Management) which covers patch management and CIP-010-1, Part 3.1 (Configuration Change Management and Vulnerability) which covers cyber vulnerability assessments."
Duke Energy	While arriving at an appropriate conclusion, this answer appears to interpret the requirement within the standard which should not be performed in this type of document. The document should limit itself to guidance and suggest eliminating the following paragraphs, "Reliability Standard CIP-007-5, Part 2.1 requires Responsible Entities to implement a patch management process for tracking, evaluating, and installing cyber security patches for high and medium impact BES Cyber Systems and their EACMS, PACS, and PCA. Part 2.2 Security Patch Management requires Responsible Entities to assess patches identified by the entity-designated source(s) within 35 calendar days. Parts 2.3 and 2.4 require the applicable security patches to be implemented within 35 calendar days or a mitigation plan developed and implemented to mitigate the vulnerabilities of each security patch not implemented within the required 35 days.

		Reliability Standard CIP-010-1, Part 3.1 requires Responsible Entities to perform cyber vulnerability assessments at least once every fifteen calendar months for high and medium impact BES Cyber Systems. The vulnerability assessment may be a documentation review or an active assessment. Part 3.2, which only applies to high impact BES Cyber Systems, requires an active vulnerability assessment to be performed at least once every 36 calendar months. Similarly, a vulnerability assessment must be performed per Part 3.3 prior to adding any Cyber Asset into an Electronic Security Perimeter containing high impact BES Cyber Systems, again limited to Control Centers. Part 3.4 requires the results of the vulnerability assessment to be documented and an action plan developed to remediate or mitigate vulnerabilities identified in the assessment." 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."
AEP		AEP supports the industry comments submitted by EEI.
Lincoln Electric		Recommend removing paragraphs 2 and 3 as they only restate what is already within the approved standard and only serves to complicate the response to the question.
ACES		For clarity, remove extra hyphen in "System Security Management" of CIP-007-5.
95	Are assets that have been in-service for years (e.g., relays installed six years ago) required to be current with security patches and does every security patch in history for the device need to be documented? If not, how far back does an entity need to go?	Responsible Entities must implement the requirements by the enforcement date. Patches before that date may be implemented as needed by the Responsible Entity but documentation is not needed before the enforcement date. Reliability Standard CIP-007-5, Part 2.1, requires Responsible Entities to implement a patch management process for tracking, evaluating, and installing cyber security patches for high and medium impact BES Cyber Systems and their EACMS, PACS, and PCA. Reliability Standard CIP-010-1 Configuration Change Management and Vulnerability, Part 2.1, requires Responsible Entities to develop a baseline configuration that includes any applicable security patches.

		For Responsible Entities in the United States, the requirements in the CIP V5 Standards applicable to high and medium impact Bulk Electric System ("BES") Cyber Systems will become enforceable on April 1, 2016.

Organization	Comments
EEI	The answer does not directly answer the question as to whether Responsible Entities are required to have all BES Cyber Systems updated ("to be current with security patches) by April 1, 2016 and every security patch prior to this date documented ("does every security patch in history for the device need to be documented"). The standard does not require all Systems to be updated by April 1, 2016, but does require a baseline configuration, which includes a listing of all applied historical and current patches. "Security patches applied would include all historical and current patches that have been applied on the cyber asset…CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches." Guidelines and Technical Basis for CIP-010-1. This documentation requirement may be burdensome for an asset that has been in service for six years and so the question as to how far back should the documentation go is reasonable. Documenting all historical patches, especially those that happened years ago will have little, if any impact on reliability. It is the patch management process itself that is important for reliability, which starts on April 1, 2016. We recommend replacing the existing answer with the following to more completely address this question: "Reliability Standard CIP-007-5, Part 2.1, requires Responsible Entities to implement a patch management process for tracking, evaluating, and installing cyber security patches for high and medium impact BES Cyber Systems and their EACMS, PACS, and PCA. The requirement also requires "identification of a source or sources" that the Responsible Entity will use for tracking the release of cyber security patches. The enforcement date for this requirement is April 1, 2016. The requirement does not require the Responsible Entity to search for historical patches to evaluate nor does it require that all BES Cyber Systems must be updated by the enforcement date. However, Reliability Standard CIP-010-1 Configuration Change Management and Vulnerability, Part 1.1, requires Responsible Entities to develop a baseline configuration, which includes any applied security patches. This baseline configuration requires documentation of applied historical and current patches (see the Guidelines and Technical Basis for CIP-010-1). Therefore Entities are expected to document the historical security patches they have applied to the BES Cyber System and their associated EACMS, PACS, and PCA as of the enforcement date."

Duke Energy	Duke Energy suggests removing the following sentences, "Reliability Standard CIP-007-5, Part 2.1, requires Responsible Entities to implement a patch management process for tracking, evaluating, and installing cyber security patches for high and medium impact BES Cyber Systems and their EACMS, PACS, and PCA. Reliability Standard CIP-010-1 Configuration Change Management and Vulnerability, Part 2.1, requires Responsible Entities to develop a baseline configuration that includes any applicable security patches. For Responsible Entities in the United States, the requirements in the CIP V5 Standards applicable to high and medium impact Bulk Electric System ("BES") Cyber Systems will become enforceable on April 1, 2016." While arriving at an appropriate conclusion, this answer appears to interpret the requirement within the standard which should not be performed in this type of document. The document should limit itself to guidance.
AEP	AEP supports the industry comments submitted by EEI.
Lincoln Electric	The question was not fully addressed. The answer given says that patches released prior to April 1, 2016 "may" be implemented. Does this mean it is up to the entity on whether to update or not update? The answer given makes it clear that documentation is not needed prior to April 1st, but is not clear on the level of patching required on relays that may have had a security patch released years ago.
Colorado Springs Utilities	CSU believes that the provided answer to this question is not helpful, as it does not answer the question regarding the need to document every available security patch in the life of an asset installed prior to enforcement of CIP v5.
Security Working Group, IRC Standards Review Committee	The SWG requests that NERC provide additional clarification regarding patch version history and associated application. Responsible Entities must implement the requirements by the enforcement date, April 1, 2016. Patches released before that date may be implemented as needed by the Responsible Entity. However, the patch version history must start upon the effective date of the Standards. Prior information regarding patch versions may be retained, but is not required – especially where such patches were not applied.

Arizona Public Service	We do not believe this response adequately answers the question. While the question is a good and sensible one, the challenge for NERC is that there is no specific language in the Standard, as currently developed, that clearly addresses how Entities should approach the grandfathering of the security patch level of devices that are in place and functioning prior to the enforcement date of CIP v5.
ACES	While the second paragraph of the provided answer is informational, we don't believe a reminder of the enforcement date is necessary.

111	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-010-1 requires Responsible Entitles to perform an active vulnerability assessment at least once every 36 months for high impact BES Cyber Systems, where technically feasible. Penetration or red team tests provide an effective means for conducting an active vulnerability assessment. That type of testing is not explicitly required by CIP-010-1, Part 3.2. As discussed in the Guidelines and Technical Basis section of CIP-010-1, less invasive testing may be performed, including active network discovery and the use of vulnerability scanning tools. Regardless of the approach used, the vulnerability assessment test should document the design and conduct of the assessment, including the Cyber Assets and networks included, the tools used, and the results of the assessment.

Organization	**Comments**
EEI	The question and answer appears to imply that the standard requires use of penetration or red team testing as an "effective means for conducting an active vulnerability assessment"; however, these active vulnerability assessment methods are not required by the standard and can cause problems if not done carefully and correctly. For example, NIST SP800-82, Chapter 3 ICS Characteristics, Threats, and Vulnerabilities, especially the Unintentional Internal Security Consequences documents specific incidents resulting from ICS scanning. Therefore the answer should make it clear that these methods are not required by the standard and refer to the references provided in the standard for further guidance. We recommend changing the answer to: "Reliability Standard CIP-010-1 requires Responsible Entities to perform an active vulnerability assessment at least once every 36 months for high impact BES Cyber Systems, where technically feasible. Penetration testing and red team tests are not explicitly required by CIP-010-1, Requirement R3, Part 3.2. As discussed in the Guidelines and

	Technical Basis section of CIP-010-1, less invasive testing may be performed, including active network discovery and the use of vulnerability scanning tools. NIST 800-115 is listed as a reference for additional guidance. Regardless of the approach used, document the design and conduct of the assessment, including the Cyber Assets and networks included, the tools used, and the results of the assessment."
Duke Energy	We suggest removing the following, "Reliability Standard CIP-010-1 requires Responsible Entitles to perform an active vulnerability assessment at least once every 36 months for high impact BES Cyber Systems, where technically feasible." In addition, we recommend adding a statement that NERC does not recommend specific tools and procedures.
AEP	As there is no specific requirement to perform neither penetration nor red team tests, AEP believes it is inappropriate to respond to the question. Further AEP does not believe it is appropriate for NERC to endorse an assessment methodology that is entirely dependent on the skill of the assessor and the agreed upon scope. The second sentence of the response should be removed. AEP believes the third sentence of the response is appropriate, "That type of testing is not explicitly required by CIP-010-1, Part 3.2", and should be expanded to explain that it is not explicitly required in any of the other CIP Version 5 requirements. Regardless of the approach used, there would need to be evidence captured and provided that sufficiently proves that the vulnerability assessment was performed and that the environment it was performed in modeled the baseline of the BES Cyber System in the production environment (CIP-010-1 R3.2.1). Additionally, documentation of the differences between the test environment where the test assessment was performed and the production environment to include how any differences were accounted for in the assessment (CIP-010-1 R3.2.2). To give advice outside of what is required, would likely create confusion and may appear to be extending requirements that are not explicitly stated, nor approved through due process.
Lincoln Electric	Agree.
Security Working Group, IRC Standards Review Committee	The SWG suggests that the response explicitly state that penetration or red team testing provide an effective means for conducting an active vulnerability assessment, but is not required. ERCOT recommends that NERC consider referencing the Guidelines and Technical Basis regarding vulnerability assessment approaches.

Arizona Public Service	This question appears to attempt to clarify whether invasive vulnerability exploitation tests – i.e. penetration testing and red teaming – are required. The wording in the Requirement column of CIP-010-1 Part 3.2.1 is very clear that the active vulnerability assessment not be performed in a production environment in a manner than can have an adverse impact. Expanding the scope of the Vulnerability Assessment requirement language to include exploitation of identified vulnerabilities with an invasive penetration test and/or red teaming exercise should be left to a SAR. The Guidelines and Technical Basis section of CIP-010-1 focuses solely on vulnerability discovery methods – not on vulnerability testing. We recommend a review of this FAQ's answer to ensure that it does not contradict the language in the FERC-approved standard and FERC Order 706 Paragraph 546 with regards to scoping of a vulnerability assessment. With regards to the second question in this FAQ, it could be more clearly worded as: "Are there specific tools or procedures that can be referenced to learn how to conduct an active vulnerability assessment?" APS believes the Guidelines and Technical Basis provides adequate guidance for a Registered Entity to begin learning how to conduct an active vulnerability assessment.

112	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 to demonstrate compliance. BES Cyber Assets may be grouped into BES Cyber Systems and assessed at the system level. Yes, paper assessments require a review of the actual configuration of the BES Cyber Asset.

Organization	**Comments**

EEI	The question has two parts that ask 1) whether a Responsible Entity can test a representative sample instead of the full population for vulnerability assessments and 2) whether a paper assessment requires a review of the actual configuration of the BES Cyber Asset. Regarding the first part, we believe the first two sentences in the answer are responsive to the question, but could be clarified. We recommend the following language: "The standard does not provide for sample testing; however, the assessments under CIP-010-1, Requirement R3, Part 3.1 applies to High and Medium Impact BES Cyber Systems 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." Regarding the second question, the answer "paper assessments require a review of the actual configuration of the BES Cyber Asset" is not accurate. Also, this simple sentence could lead to a potential double jeopardy for noncompliance. CIP-010-1, Requirement R3, Part 3.1 requires a paper or active vulnerability assessment and elements of paper vulnerability assessments are described further in the Guidelines and Technical Basis for CIP-010-1. However, the measures for this requirement are limited to the documentation of the assessment, the controls assessed, and the method of assessment used. If during a paper vulnerability assessment, a Responsible Entity determines that an enabled logical port no longer has an appropriate business justification, then the entity is not found in violation of CIP-010-1, R3, but must, if technically feasible, disable or restrict the logical access to the report under CIP-007-5, R1, Part 1.1, to be compliant with CIP-007-5, R1, Part 1.1. We recommend changing the answer to the second part of the question to: "To demonstrate compliance with CIP-010-1, Requirement 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-010-1."
Duke Energy	The last sentence needs to be removed as this is introducing a requirement that does not exist in the current Standard/Requirement language.

Georgia Transmission	GTC appreciates the opportunity to provide comments on these outputs from the V5 Transition study. With respect to FAQ #112, the standard does not preclude testing a representative system for identically configured systems. The standard only states "At least once every 15 calendar months, conduct a paper or active vulnerability assessment." The question did not ask if a random sampling could be used. Conducting thorough testing on a single device and then validating that other devices are identically configured to the tested device is an ideal way to deal with the extremely large number of devices that operate in substation and generation environments. Additionally, the standard never states that a paper assessment requires a review of the "actual configuration of the BES Cyber Asset." While we do not currently know a way to conduct a paper assessment without doing this, we feel that it is completely inappropriate for this FAQ to specify a requirement. The response could state that "paper assessments are typically conducted as a review of the actual configuration." Preferably, the FAQ should just refer to the existing guidelines and technical basis section of CIP-010 to identify recommended elements to include in a paper vulnerability assessment.
AEP	The wording of the question introduces terms not properly addressed by the terms adopted by the NERC CIP standards. Is the questioner conflating "identically configured populations" as Cyber Assets that share an identical configuration? If so, is NERC suggesting that those Cyber Assets should be grouped into a BES Cyber System and tested as a whole? If so, and we believe this is the intent of the question, does each component Cyber Asset need to be tested?
Lincoln Electric	Please clarify if during a vulnerability assessment all BES Cyber Assets must have their actual configuration reviewed. Also, please detail what the configuration is to include. Can the Vulnerability Assessment be performed at the BES Cyber System level?
Colorado Springs Utilities	CSU believes the provided answer to this question is not helpful, since requiring a review of the actual configuration of the BES Cyber Assets in a BES Cyber System appears to preclude the use of a system grouping for sampling purposes. The answer would be clearer and more helpful if the second sentence was deleted.
Entergy	Identically configured devices would possess the exact same vulnerabilities, if any. For a paper vulnerability assessment, reviewing the documentation/testing 50 devices that are identically configured offers little to no increased risk reduction or vulnerability identification over testing a sample of the device type/configuration. The value for Active CVA's on all Cyber Assets is clear, but for a paper work exercise it offers little to no benefit and will

	only serve to further stretch entity resources unnecessarily as workers review hundreds or thousands of identical documents.
Arizona Public Service	NERC's answer to the FAQ is inconsistent with the methodologies implied in CIP-010 R3.2 for performing vulnerability assessments in a test environment. CIP-010-1 R3.1, which includes Medium assets, specifically permits the Entity to choose between a paper or active assessment, but lacks the elaboration CIP-010-1 R3.2 has on the conduct of an active assessment – more specifically, that the active assessment can be conducted in a test environment – an environment which, in NERC's language, can "model" the production environment. NERC's Glossary of Terms (as updated May 19th, 2015) does not provide a definition for the word "model" or "modeling", but the clear intent is to allow the Entity to more safely perform a vulnerability assessment in a laboratory environment so that the potential of harm to the BES is greatly reduced or eliminated. If the assessment is active, the statement that there is no room in the standard for sample testing is in conflict with both CIP-010-1 R3.2 and the spirit of reducing or eliminating the risk of harm to the BES.

113	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-010-1 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 and CIP-007 are not adversely affected." Responsible Entities may choose how they test patches to ensure the cyber security controls required by CIP-005-5 and CIP-007-5 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.

Organization	**Comments**

EEI	We support this question and answer.
Duke Energy	We believe that a yes/no response is needed on whether a quality assurance environment is necessary. The response provided does not adequately answer the question asked.
AEP	AEP supports this response.
Lincoln Electric	Agree.

114	How have the requirements for testing changed from Version 3 of the CIP Reliability Standards, to Version 5?	In response to FERC Order No. 706 directives, the standards drafting team revised CIP-007-3 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." These changes are reflected in CIP-010-1 R1.4 and R1.5. Both requirement parts require testing for "each change that deviates from the existing baseline configuration" in R1.1. Both requirement parts require determining which "required cyber security controls in CIP-005 and CIP-007" could be "impacted by the change" and verifying after a change that those controls were "not adversely affected." Additionally, CIP-010-1 R1.5 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 BES Cyber Systems in the production environment may be used for testing. If a test environment is used for R1.5, refer to specifics in R1.5.2 for required test environment documentation.
Organization		**Comments**

EEI	We support this question and answer.
Duke Energy	While the answer provided focuses on testing as it appeared in one requirement in V3, the question is not specific enough to warrant limiting the answer to just this requirement. Testing appears in multiple other requirements in CIP V3 (patching and anti-virus amongst others) and the answer should support each of these equally (or limit the scope of the question specifically).
AEP	AEP supports this response.
Arizona Public Service	This question is too broad to be considered informative. Recommend it not be considered for inclusion in a FAQ.

21	Substations with external IP routable connectivity require that all cyber assets are determined to be BES Cyber Systems or Protected Cyber Assets. Please confirm that Protected Cyber Assets does not apply for substations without External Routable Connectivity.	Reliability Standard CIP-005-5, Requirement R1 requires applicable BES Cyber Systems connected to a network via a routable protocol to have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. A Cyber Asset becomes a Protected Cyber Asset (PCA) when that Cyber Asset is within an Electronic Security Perimeter associated with a high or medium impact BES Cyber System regardless of whether there is External Routable Connectivity. There are several requirements in the Reliability Standards that are applicable to "Medium impact BES Cyber Systems and their associated PCA". These requirements apply to those BES Cyber Systems identified at a substation that are within the same ESP as a high or medium impact BES Cyber System without regard to External Routable Connectivity.

Organization	**Comments**
EEI	The existing question and answer mixes the terms External Routable Connectivity, Protected Cyber Assets, and Electronic Security Perimeters such it is confusing to the reader. To make this FAQ useful we recommend changing the question and answer to the following:

	Q: “Are Electronic Security Perimeters and Protected Cyber Assets applicable to all Medium Impact BES Cyber Systems at transmission substations and does External Routable Connectivity impact this applicability?” A: “Reliability Standard CIP-005-5, Requirement R1, Part 1.1 requires Medium Impact BES Cyber Systems and their associated PCA “connected to a network via a routable protocol to reside within a defined Electronic Security Perimeter (ESP).” For transmission substations with 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 according to CIP-005-5 R1, Part 1.1 reside within a defined ESP and the Protected Cyber Assets (PCA) definition may be applicable to Cyber Assets at the substation. However, if a Medium Impact BES Cyber System and its applicable Cyber Assets in a substation are not connected to a network via a routable protocol, then CIP-005-5, Requirement R1, Part 1.1 does not apply, a defined ESP is not required, and the PCA definition does not apply because there is no ESP. A Cyber Asset becomes a PCA when that Cyber Asset is “connected using a routable protocol within or on an Electronic Security Perimeter” associated with a high or medium impact BES Cyber System regardless of whether there is External Routable Connectivity. There are several requirements in the Reliability Standards that are applicable to "Medium impact BES Cyber Systems and their associated PCA". These requirements apply to those BES Cyber Systems identified at a substation that are within the same ESP as a high or medium impact BES Cyber System without regard to External Routable Connectivity.
Duke Energy	The question needs to be revised to correct a critical error. The question states that substations with external IP routable connectivity require that all cyber assets are determined to be BES Cyber Systems or PCAs. This statement is flawed as not all cyber assets will be BES Cyber Systems (depending on performing a BES Cyber Asset assessment) or PCAs. There is the potential that some Cyber Assets at that location will not be BESCS or PCAs. This should be corrected in the question or the answer provided in addition to the response given.
AEP	AEP supports the industry comments submitted by EEI.
Lincoln Electric	Agree.

Colorado Springs Utilities	CSU believes that this answer would be more complete if it also addressed situations where the only communication protocol internally and externally to the Substation is non routable (serial).
Entergy	Entergy proposes the third sentence to read as "A Cyber Asset becomes a Protected Cyber Asset (PCA) when that Cyber Asset is connected using a routable protocol within or on an Electronic Security Perimeter associated with a high or medium impact BES Cyber System regardless of whether there is External Routable Connectivity." This more closely follows the definition of Protected Cyber Asset in the NERC Glossary of Terms, as noted below, and adds additional clarity to the response to the question. PCA's are not concerned with the External Routable Connectivity capability of the ESP, as noted in the response, but with the connectivity of the Cyber Asset to the ESP and/or BCS. A PCA must be connected with a routable protocol. "Protected Cyber Assets – One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."
Arizona Public Service	This response seems to be at odds with the definition of "Protected Cyber Asset" from NERC's Glossary of Terms, as of the May 19, 2015 publishing: One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The answer to this FAQ has removed the routable protocol usage from consideration. Regardless, it is difficult to understand the intent behind this question. APS recommends it be stricken.

	If the question is reworded to provide clarity, APS recommends the answer be appropriately clear to the reworded question and not contradict the published record.