NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Questions and Answers

CIP Version 5 Standards

Version: June 13, 2014

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

This document provides answers to questions asked by entities as they transition to the CIP Version 5 Standards. The questions are listed by the CIP Version 5 standard requirement they are associated with, and will be updated periodically throughout the Transition Period as new questions arise. More complex topics are addressed separately in a series of Lesson Learned documents developed by NERC.

Technical Questions and Answers - CIP Version 5 Standards	
Question	**Answer**
General	
CIP-002-5 BES Cyber Systems Categorization	
1. In reference to the Cyber Security Standards Transition Guidance, if an entity opts to utilize its Version 3 Risk Based Assessment Methodology, how will an audit treat Black Start and Cranking Path resources during the transition period?	The primary goal of the transition guidance is to ensure that grid reliability is adequately protected as intended by compliance with the CIP Version 5 Standards and without forcing a Responsible Entity to exert undue effort on satisfying requirements that are, in effect, becoming obsolete or superseded. The guidance that has been provided is not only applicable to Responsible Entities but also to ERO auditors; thus, auditors no longer consider whether Black Start and Cranking Path resources are potential Critical Assets.
2. What documentation / evidence would an entity need to demonstrate why selected Critical Assets were removed from their Critical Asset list if it opted to utilize its Version 3 Risk Based Assessment Methodology?	An auditor would expect to see evidence that supports the designation of assets throughout the audit period. For the period of time when the Critical Asset list was derived from the application of an RBAM, the effective dates of the methodology and the resulting list(s) would be necessary.

Technical Questions and Answers - CIP Version 5 Standards

Question	Answer
	When the Critical Asset identification method changes to one of the alternative approaches described in the "Cyber Security Standards Transition Guidance", supporting documentation also would be expected to reflect that. A Responsible Entity must identify the approach it is using for asset identification, but the method for documenting that approach is at their discretion; for example, a policy, a memo, or other corporate document. Whatever form the documentation takes, however, it should indicate when the approach was in effect and the list of Critical Assets that resulted.
3. NERC draft Transition Guidance dated July 2013 indicated that an entity removing assets "…may do so only after their Reliability Coordinator, Transmission Planner, Planning Coordinator, or Planning Authority confirm notification of the removal." September 2013 NERC Transition Guidance indicates 3rd parties are responsible for reaching out (vs. the entity): "NERC highly encourages these third parties to proactively designate the necessary assets in a timely fashion." What is the expectation related to notifying the Reliability Coordinator, Transmission Planner, Planning Coordinator, or Planning Authority?	NERC has not specified a time period or details for correspondence between the Registered Entities and related third parties. However, we expect that the Responsible Entity will provide ample correspondence with the third party's relevant personnel. This correspondence could include requests from the Responsible Entity to the third party regarding the assets being considered for removal, third party responses, or relevant studies.
4. We have a control building inside a substation that is considered to be a Medium impact rating. A transformer has a port on it that provides data to the protected systems inside the control building. Would the transformer port need to be protected under the CIP Version 5 standards?	The transformer port would need to be examined to determine the nature of the connection. If there is any bi-directional data flow through the port, it could be vulnerable to intrusion. The port would be within the Electronic Security Perimeter of the control building systems and therefore would need to be a Protected Cyber Asset (PCA).
5. What exactly needs to be protected in substation yards and generation plants? We have a few devices located in the yard of a substation and are not sure if they are in scope for protection. These include: a) Transformer monitoring devices b) Distribution Relays c) Monitoring PLCs d) HMI Workstations that control non-critical assets (soot blowers, water cannon, etc.). We are also wondering about the data that is generated from these devices; should that be protected/encrypted?	In general, if a device plays a role in BES reliability or operations, or would be considered a PCA because of network connectivity, then it needs to be protected according to its impact rating (Medium or Low). It may be helpful to review the definitions of BES Cyber Asset and BES Cyber System to verify whether a device meets the criteria. A key consideration is to assess when and where generation or transmission facilities are tied together electrically, such as at a distribution interconnection point. When such facilities are tied together electrically, they need to be considered together because ties between low and high sides may mean a device could take out a

Technical Questions and Answers - CIP Version 5 Standards

Question	Answer
If so, will it make any difference if the data is read-only and there is no way for the data stream to make modifications to the end-point?	transformer. Thus, with that level of impact on the high side, it is brought into scope. While encryption is a good security practice, it is only required for Interactive Remote Access. Read-only vs. read-write is not the issue; rather, determine whether the communications protocol could be compromised (if routable), or if the data is used upstream to make operational decisions. If either of these circumstances exist, then the devices need to be protected. Even read-only devices that use a request-response protocol use bi-directional communications.
CIP-003-5 Security Management Controls	
1. We are trying to determine the methodology behind the Identify, Assess and Correct (IAC) portion of the requirements. Our current thought is that once the policies and procedures are put into place, we will need to design auditing tests to verify that the policies and procedures are working as designed. If we find any abnormalities, then we will assess how best to fix the problems and then put those changes into place. The evidence for compliance will be the tests that were designed, as well as the results on the sample data.	Since the IAC language is likely to be removed from the CIP Version 5 Standards as directed by FERC, this response provides a perspective from a Reliability Assurance Initiative (RAI) approach to compliance and enforcement: Actions that demonstrate an effective compliance regimen will be useful evidence to have available during an audit. For example, the controls in place for timely detection of noncompliance, the controls in place to detect the underlying noncompliance, the timely assessment and remedying of the noncompliance, and the documentation of each noncompliance and its remediation all reflect a proactive and mature approach to managing risk.
2. Do the CIP Version 5 standards (CIP-003-5 R3) require that the CIP Senior Manager be identified and documented again, if that is already in place under Version 3?	No, the CIP Senior Manager does not have to be re-identified, provided the existing documentation meets the CIP Version 5 standard requirements.
CIP-004-5 Personnel & Training	
1. We are looking for guidance/clarification concerning CIP-004-5 Table R2, Part 2.1 - Requirement 2.1.9, “Training Content on Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets.” Is this requiring that the training will cover the dangers of, for example, adding a new device to the protected network whether authorized or unauthorized? Perhaps it covers generally the interdependence of all networked devices and their vulnerability to inadvertent as well as malicious	Consider the audience and what they have access to and are capable of doing – knowingly, unknowingly, accidentally, or maliciously. The training should discuss the risks associated with the particular asset(s) that the audience interacts with. For example, if the audience is control room operators, then training could focus on HMIs that are used to perform work and risks associated with that environment: attaching USB devices, changing Ethernet cables with nearby devices,

Technical Questions and Answers - CIP Version 5 Standards

Question	Answer
changes? Without some guidance, this statement could easily be interpreted so broadly as to paralyze any effort to document it.	modifying or attempting to modify security or network settings, etc.
CIP-005-5 Electronic Security Perimeter(s)	
CIP-006-5 Physical Security of BES Cyber Systems	
CIP-007-5 System Security Management	
1. What are the checks and monitoring (e.g., logging requirements, anti-virus, active ports) required for new Field Devices? (in substations or generation plants) a) PLCs b) Relays c) Monitoring devices	The standards do not distinguish between Cyber Asset types. Start with the applicability of the standard; if the device capability is there, then respond and implement accordingly. Be cognizant of differences between the requirements for high and medium impact BES Cyber Systems.
CIP-008-5 Incident Reporting and Response Planning	
CIP-009-5 Recovery Plans for BES Cyber Systems	
CIP-010-1 Configuration Change Management and Vulnerability Assessments	
1. How are we going to define "baseline" on protected assets? CIP-010-1 R1, Part 1.1 identifies five items that make up the baseline for protected assets: software/firmware versions, open source/commercially available software, custom applications, logical network accessible ports, and applied security patches. What else will be part of the baseline: configuration settings (IP addresses, thresholds for the monitoring devices, etc.), or any hardware differences (such as video cards, CPUs, memory capacity, etc.)?	The five items identified in CIP-010, R1, Part 1.1 are the minimum requirements for establishing and maintaining a baseline, and are likely to be checked during an audit. Information about hardware differences (e.g., the video card noted) may apply since it could affect installed applications and patches. Other information (e.g., IP address) may be useful but not required in the baseline configuration since it differs from node to node. While a baseline is typically considered in the context of servers and other IT equipment, it also applies to BES Cyber

Technical Questions and Answers - CIP Version 5 Standards

Question	Answer
For example, if the addressing on a relay is changed, or the amount of oil in a transformer that a device is monitoring was modified, would this cause a new baseline to be created? The relay or device itself would not change, just one of its monitoring/alarm thresholds.	Assets such as relays. Configurations for BES Cyber Assets are not specifically addressed by the items that are mentioned in the requirements. An example of an approach to evaluating the criticality of a BES Cyber Asset setting is to assess the impact that would result from the loss of that setting.
2. Are configuration changes to protected assets covered in CIP-010-1? Will any and all configuration changes to monitoring thresholds, addressing changes, or any other change to a specific device that is not part of the 5 baseline items, be in scope for the change management portions of CIP-010-1? Similarly, for the hardware inside a protected asset would a change to the amount of RAM or adding drives to a PCA force us to create a new baseline?	The standard specifically addresses changes to the baseline only. However, good management and security practices would include other changes, such as hardware changes, as well.
3. What exactly is the definition of “security” patches in CIP-010-1, R1, Part R1.1.5? There are patches that are labeled as Critical, Important and Security; which of these (or any other designations) fall under the umbrella of CIP-010-1 “security” patches?	Requirements pertaining to security patches are addressed in the same manner as in previous versions of the CIP standards. The concept is to distinguish “security” patches from “functionality” patches. The standards are focused on security patches, no matter how that description is communicated by the vendor. Words like “critical”, “important,” or “security” are likely good indicators that a patch should be considered a security patch. Also be aware that patches themselves may address multiple types of issues, and many (and perhaps most) vendors will not label a patch as being limited to “security” issues. That is especially true for an appliance-type update, which could include security functions within it.
4. Two computers/servers/devices have the same items in each of the five baseline requirements, but have only one difference (e.g., an additional application or an applied patch). Will this cause a new baseline to be created and therefore require a change to the baseline documentation?	In this example, since installed applications and patches are part of the baseline, then a new baseline would be required. Changes that are not part of the baseline (e.g., an IP address) do not require a new baseline.
5. Will non-protected cyber assets fall under the baseline, and if so, how do we meet this requirement? For example, desktop computers that are used to access Active Directory to add/modify/remove users or to change the logging/alerting thresholds on the monitoring servers are currently labeled as “non-CCAs” within the ESP. How will these computers/devices be treated under CIP Version 5?	If the Cyber Assets are inside an ESP, they are Protected Cyber Assets and are required to have baselines (see the applicability column of CIP-010-1, R1, Part 1.1).

Technical Questions and Answers - CIP Version 5 Standards	
Question	**Answer**
6. Do monitoring clients and their agent's configuration file need to be included in the baseline as required in CIP-010-1?	A monitoring client that is an installed application should be included in the baseline. The agent's configuration file is not part of the auditable baseline, but should be documented. Note that the baseline can also be used to streamline the patch analysis process and the rebuilding of any nodes that are replaced. Anything that can help that process should be documented, even if not subject to audit (e.g., perhaps a high-level baseline for audit purposes, and a separate more detailed baseline or configuration document that might contain related configuration information, IP addresses, etc.)
7. CIP-010 R3.1: Perform active assessment(s) for all transmission substations using assets in a test lab. Can entities perform active assessment(s) which would cover all assets used in transmission substations using a test lab? Will the entities be required to perform assessments on each individual transmission substation? Note that entities may have many different transmission substations categorized as medium impact BES Cyber Systems under CIP Version 5.	Entities may perform active cyber vulnerability assessments in a test lab as long as the differences between the production environment and test environment are documented. The evidence must show that each asset type in the transmission substations is represented in the test lab. The assessment process must address how the lab remains current with substations as they undergo equipment changes, upgrades, architecture modifications, etc. Note that CIP-010-1 R3, Part 3.2 requires active vulnerability assessments of high impact BES Cyber Systems. CIP-010-1 R3, Part 3.1 allows either paper or active assessment.
8. CIP-010 R3.1: Perform separate PACS and EACMS assessments. Can entities perform separate assessments for PACS and monitoring (EACMS) assets? Or must all PACS and monitoring assets be included in individual BES Cyber System assessments? Note that some entities utilize centralized cyber security monitoring systems and PACS with distributed infrastructure, with some PACS and monitoring assets located in corporate data centers, and other PACS and monitoring assets co-located with the BES Cyber System.	CIP Version 5 requires that all the systems identified in the Applicable Systems column are assessed. It does not specify how the assessment is to be performed or how the systems must be grouped. BES Cyber Assets may be grouped into systems to help facilitate the assessment. For example, it may be helpful to assess an EMS BES Cyber System that includes PACS and EACMS as one system. However, an EMS BES Cyber System, a PACS BES Cyber System, and an EACMS BES Cyber System may be assessed separately.
9. CIP-010 R3: Low Impact BES Cyber System assessments. Will entities be required to perform assessments of low impact BES Cyber Systems?	The CIP Version 5 standards do not require cyber vulnerability assessments on low impact BES Cyber Systems. The applicability sections of CIP-010-1 R3 only address high and medium impact BES Cyber Systems and their PACS, EACMS, and PCAs.

Technical Questions and Answers - CIP Version 5 Standards	
Question	**Answer**
10. CIP-010 R3.1 and R3.2: All assets. Can entities perform assessments on groups of like assets (type-based assessment) or must entities include all assets in assessment activities? Does this apply to both paper and active assessments?	Cyber vulnerability assessments may be performed against a representative cyber asset, generally based on utilizing a common baseline configuration. Cyber Assets that have different baseline configurations, or where baseline configurations are augmented with additional software or configuration changes, must be assessed separately. It may be more practical to assess the assets on the basis of how they are grouped as systems. All Cyber Assets need to be assessed regardless of which baseline and comparison is used.
11. Are entities expected to perform an assessment of all BES Cyber Assets or should the testing be done at the BES Cyber System level?	CIP Version 5 is intended to apply to the BES Cyber System. Since a BES Cyber System contains one or more BES Cyber Assets, an active assessment would include each individual BES Cyber Asset. A passive assessment must account for different baseline configurations or when baseline configurations are augmented or modified.
12. CIP-010 R3.1: Paper assessment. Is the paper assessment a "document review" exercise, or does CIP Version 5 require that physical inspections, enumeration of ports and services, and similar activities be included within the scope of the paper assessment?	The intent of the "paper" assessment is to include document reviews (e.g., reviews of known vulnerabilities of installed software) as well as dumps of configurations (e.g., a list of open listening ports generated by platform-resident tools such as netstat). For example, a paper assessment could contain information about issues such as current threats and how the baseline configurations are designed to address them.
13. CIP-010 R 3.2: Active assessment Are tools such as Nmap required for active assessments, or can entities use custom scripts (which use native OS commands) to enumerate open ports and services? What constitutes an active port scan?	Commonly used tools such as Nmap are preferred to conduct active vulnerability assessments to ensure that the assessment is accurate and complete. Custom scripts using native OS commands could be corrupted (e.g., modified not to show all open ports). Also, entities will need to provide evidence that custom scripts have been properly designed, developed, and tested so that the results of the assessments may be validated. The intent of the active assessment is to test the Cyber Asset from the "outside" rather than simply having the Cyber Asset look at itself.
14. CIP-010 R3: Separation of duties What level of independence is required of the vulnerability assessment team members? Can individuals who are responsible for maintaining BES Cyber Asset configurations also be responsible for performing vulnerability assessments? Can testing be performed internally by the entity or is there a preference for external third-party assessors?	CIP Version 5 does not require the use of third parties to conduct cyber vulnerability assessments. However, using a combination of internal, external, and non-affiliated third-party evaluators would be an example of an effective management practice. An external assessment by individuals who have no role in maintaining or configuring the systems on which the

Technical Questions and Answers - CIP Version 5 Standards

Question	Answer
	vulnerability assessment is being performed is recognized as a good security practice.
CIP-011-1 Information Protection	
1. With all of the new devices coming into scope for CIP Version 5, what types of documentation will come into scope for document security? a) Configuration sheets b) Engineering drawings of BES substations c) Relay addressing sheets d) Other documentation	The definition of BES Cyber System Information can help with identifying the required minimum levels of protection. Keep in mind that the definition applies to the metadata about BES Cyber Assets/Systems, not to the power system data that they contain. This definition of BES Cyber System Information is from the NERC Glossary: *"Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to: security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System."* While appropriate protection is essential, it is also necessary to avoid overprotection that will create unintended consequences; e.g., relays with setting information that is deemed to be BES Cyber System Information will make it unnecessarily difficult to make repairs.