NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions

CIP Version 5 Standards

April 1, 2015

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 or to modify the requirements in any existing Reliability Standards. The ERO Enterprise will continue to determine compliance based on language in the NERC Reliability Standards, which may be amended in the future.

NERC is soliciting industry feedback on the draft answers listed below. NERC will review all comments provided and incorporate changes before issuing a final version of the April 1, 2015 FAQs.

Instructions: Please type comments directly into this document in the white rows labeled "Comments" under one or more of the questions and answers below. Commenters need not provide comments under each question and answer. Send the completed Word document to TransitionProgram@nerc.net by May 15, 2015.

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

Number	Question	Answer
22	Is RFC 1490 Protocol considered serial? Routable?	A communications protocol that contains a network address as well as a device address is typically defined as a routable protocol. TCP/IP is a routable protocol, and the IP network layer in TCP/IP provides this capability. The TCP/IP suite provides two transport methods. TCP ensures that data arrive intact and complete, while UDP just transmits packets. RFC 1490 is an encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. If IP traffic is encapsulated in this protocol, then it would be considered to be a routable protocol. Frame relay itself is a communications protocol that creates Permanent Virtual Circuits

		(PVCs) to send traffic between locations. Once PVCs are created, the network communications more closely resemble layer 2 communications. Examples: 1. If it is bridged to operate similar to a VLAN, then it is routable (but may possibly be considered similar to a layer 2 switch). 2. If it is used as an end-to-end IP link, then it is routable (but is evaluated differently since it is layer 3). 3. It can also be considered a communication link transport media, but that doesn't really change anything. The entity would need to evaluate to see if the communications would qualify for exemption under Section 4.2.3.2 under CIP-002-5.
Comments:		

23	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.
Comments:		
25	Should the identity management tool be classified as an EACMS? It will reside in an ESP DMZ environment and could be on a dedicated VM infrastructure.	The definition of Electronic Access Control or Monitoring Systems (EACMS) is "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." If the function of the identity management system is to capture and/or gather information pertinent to the attributes (e.g., biometrics) of a subject or data relevant to a subject, then perform a subsequent analysis or decision of the captured data to enforce access control (e.g., authentication and/or authorization) or monitoring of an Electronic Security Perimeter, then the identity management system should be considered an EACMS.
Comments:		

33	When identifying BES Cyber Systems, what is the definition of adverse impact?	Per comments from the standards drafting team, an adverse impact is a negative effect on the reliable operation of the BES. (See bottom of page 60 in the comments link provided above.) Entities need to perform some work to determine situations that would have a negative (adverse) impact on their normal (functional) operations. While we can produce specific examples, every entity is different, so adverse impact may have a different meaning to each.
Comments:		
45	How do you define 1500 MW?	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 generation units. The following should be used for determination of Net Real Power: • Any method approved by a Transmission Planner or Reliability Coordinator that is independent of the Generator Owner. • Industry accepted engineering studies of net generation output, such as may be required of market participants. • The highest aggregate net generation output for the prior two years from an entity's energy accounting software. Reference MOD-024/MOD-025 as an acceptable approach.
Comments:		

49	What is a “shared” BES Cyber System?	One that affects two or more BES Facilities, such as multiple generation units. Reference the use of "shared" in context as used in CIP-002-5.1, Attachment 1, impact rating criterion 2.1.
Comments:		
50	What are “common mode vulnerabilities?” – i.e. a (physically) control room that can control multiple units, a substation/yard for a power plant	Any systems that can affect two or more BES Facilities, such as multiple generation units. A substation could affect the entire generation location if it were disabled and power was not able to be transmitted on the grid. Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities. Refer to the Generation Segmentation Lesson Learned document.
Comments:		
52	How can we show that there is not a 15 minute impact on BES (what evidence needs to be supplied)?	Reference the BES Cyber Asset Survey for an indication of the types of systems the Implementation Study participants identified.
Comments:		

54	Where in the standards is the FERC Order 706 directive on joint ownership or joint use addressed?	Since one Registered Entity must be responsible for compliance, there will need to be an agreement (e.g., JRO, CFR, MOU) in place clearly stating which Registered Entity has responsibility. Guidelines and Technical Basis states: "It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards." There is not an obligation in the CIP standards to have JROs, CFRs, or MOUs. Registered Entities can also get best practices ideas from peer forums, such as the Transmission Forum, the Generator Forum, and/or regional compliance forums.
Comments:		
55	What are the complete requirements for BES Cyber Systems without routable or dial-up access?	Refer to the applicability section of each standard.
Comments:		
58	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 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.

Comments:		
62	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. The CIP Exceptional Circumstance is listed in six requirement parts. In the instance of a CIP Exceptional Circumstance, the Registered Entity provides evidence that a CIP Exceptional Circumstance has taken place and the timeframe it temporarily suspended compliance with any of those six specific requirement parts. 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.
Comments:		
63	Does the standard require separate training for each role, function, or responsibility? "	No, all nine elements have to be covered, but a separate course is not required for each.
Comments:		
64	For revocations and transfers, what is the initiating action or when does the clock start for immediate, 24 hours and next calendar day?	From the CIP-004-5 Guidelines and Technical Basis: "This requirement recognizes that the timing of the termination action may vary depending on the circumstance." The guideline goes on to specify possible processes associated with termination scenarios. The clock starts on revocation when the entity takes action to terminate according to their process. The 24 hour clock starts on the company-determined termination action for terminations and should be completed within 24 hours. For transfers, the revocation must occur by the end of the next calendar day in which a company decides the individual no longer needs access. Business days are not taken into consideration for this Requirement. Entities should be careful to observe these timeframes even on weekends and holidays. An action to terminate could be the notification to the individual of their termination.

Comments:		
77	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. Because 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/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.
Comments:		
80	If Part 1.4 (Dial Up Connectivity) applies, what other standards have to be applied to that device? Does it revert back to all Medium Impact standards? Or just this one?	Dial-up connectivity is a specific connection mechanism applied to High and Medium Impact BES Cyber Systems under CIP-005 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.

81	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 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.
Comments:		
82	Regarding CIP-005-5, page 17, 2nd paragraph in the Guidelines for R1, are serial ports exempted from the ESP consideration? Can the serial communications extend beyond the 6 walls of the PSP as long as they are terminated inside another PSP? The example is for a substation with multiple control houses with buried fiber cables between the two houses carrying serial signals.	No requirements are applicable.
Comments:		

83	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 requirements for the revisions to CIP-006-5?	Entities can determine how they want to define their ESPs. For the CIP-006-6 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. This requirement does not apply to substations.
Comments:		
84	For CIP-005-5 R1 Part 1.1: for a medium impact BCS at a substation that is connected via serial communications to the EMS. Inside the substation control room, there is an HMI with a LAN that communicates inside the substation over IP. The language in the standard says "All applicable Cyber Assets connected to a network via routable protocol shall reside within a defined ESP." Which network does "a network" refer to?	Without knowing the architecture, the following response indicates the minimum that should be done: There are two networks defined here: The communications network back to EMS and the substation internal network. Because the internal network is routable, there would be a need to create an ESP (as well as a PSP) around the internal network. The guidelines and technical basis entry states: “All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP.”

Comments:		
86	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)..."
Comments:		
89	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 (even if the badging station location is a low impact facility)?	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 Systems. As such, the PACS Cyber Assets have protections that must be applied according to the specific requirements of CIP V5 and should assume the protections required for the highest rated BES Cyber System with which it is associated.
Comments:		

90	What does the testing requirement in CIP-006-5, 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". 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. PACS workstations functional tests include, but may not be limited to, granting, revoking, monitoring, and logging of access.
Comments:		
91	"(M)onitor…for unauthorized physical access" for the individual devices that make up the PACS system. Or is this directed to the servers that host the PACS? Do you need to alarm/alert on each of the guard and badging workstations?	Yes, the physical access to the PACS servers, controllers, and guard and badging systems is monitored and alerted on for potential unauthorized access. In accordance with CIP-006-6, R1, Part 1.6, all devices that make up the PACS system including servers, controllers, and workstations should be brought into scope for this requirement.
Comments:		

92	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 (e.g., Nessus Credential Scans). • 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.
Comments:		
93	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 should adhere to the entity's CIP-011 Information Protection program.
Comments:		
94	Signage for physical port protection (CIP-007-5, 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 signage is used, the sign (in the appropriate language for the Responsible Entity) must be as close to the applicable port as possible to be effective to deter inappropriate use of the port.
Comments:		

98	For CIP-007-5 R3 Part 3.1 on malicious code for non-routable sites, is hardening or group policy sufficient?	“System hardening," "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". While 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.
Comments:		
101	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?	Devices that utilize passwords without an associated user ID must be included in the registered entity’s inventory of default and generic accounts. 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 in the applicable systems column, 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.
Comments:		

107	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? 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-010-1, 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-007-5, R1, Part 1.1. Response 2: Penetration testing is not required for CIP-010, but an active vulnerability assessment is an option under CIP-010-1, R3, Part 3.1, and a requirement under CIP-010-1, R3, Part 3.2. An active vulnerability assessment is described in the Guidelines and Technical Basis section of CIP-010-1, R3. For a discussion on a similar topic, see also FAQ #111.
Comments:		
108	How should active vulnerability scans be managed for PACS systems given their sensitivity to Denial of Service?	CIP-010, 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 its PACS susceptibility to Denial of Service attacks. For instances, if the PACS is highly susceptible to Denial of Service attacks, then the entity should only conduct paper vulnerability assessments. Although an active vulnerability assessment is required every three years for a high impact BES Cyber System, this does not apply to PACS.
Comments:		
128	For v3 Critical Assets and associated Critical Cyber Assets that will be classified as low impact BES Cyber Systems under v5, what is expected for declassification and destruction of	If the information is specific to the asset, then information pertaining to that asset is also declassified and will be subject only to the entity's normal information security policies. If the information on the declassified asset includes information on other assets that will not be declassified, the information will need to be treated as BES Cyber System Information.

	critical information if the facility remains in operation?	
Comments:		
129	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 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 R2.1, which address the reuse of Cyber Assets. If the device is not released 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. Responsible Entities should keep in mind that not all data requires protection under the CIP standards. Responsible Entities should evaluate whether the Cyber Asset contains any data that should be classified as BES Cyber System Information or any critical energy infrastructure information (CEII) and protect the information accordingly.
Comments:		

130	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. The Responsible Entity should ensure that the media containing BES Cyber System information cannot be retrieved in any way. Procedures should be tested to ensure that the method(s) used achieves the goal of destruction. Degaussing and 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.
Comments:		