CIPv5 NESCOR/NESCO/EPRI Comments

January 6, 2012

The following tables include NESCOR/NESCO/EPRI comments on the draft version 5 of the NERC CIPs. The comments were developed by members of the NESCOR and NESCO teams. The following individuals contributed specific comments:

Contributor	Organization
Annabelle Lee	EPRI
Marc Child, Scott Hughes	GRE
Andrew Wright	N-Dimension Solutions
Chan Park	N-Dimension Solutions
Dan Widger	N-Dimension Solutions
Stacy Bresler	NESCO
Carol Muehrcke	Adventium Enterprises
Josh Axelrod	AlertEnterprise!
Mladen Kezunovic	TLI
Tomo Popovic	TLI
Art Conklin	University of Houston (UH)
Glen Chason	EPRI

Elizabeth Sisley	Calm Sunrise Consulting
Scott Sternfeld	EPRI

CIP xxx-5 General

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
implementation plan	49	Andrew Wright, N-Dimension	The implementation plan calls for CIPv5 to come into effect January 1, 2015. Given that this draft has already been in the works for nearly two years, it is not clear why the effective date is three years in the future.
several	4	Chan Park & Andrew Wright N-Dimension Solutions	For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…", this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for "every 39 months…". To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z".
Definitions	1	Carol Muehrcke Adventium	Clarify definition of Electronic Access Point Electronic Security Perimeter – definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts".
		Annabelle Lee (EPRI)	As stated in the document, "...from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets." Why are only cyber assets listed and cyber systems excluded? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Stacy Bresler NESCO	single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." The term *element* is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. BES Cyber System mentions the phrase Maintenance Cyber Asset. This phrase has no associated definition. There is no explicit reference to generator control rooms in the definition a Control Center. It should made clear if a generator control room is included or not.
several	1	Elizabeth Sisley, Calm Sunrise Consulting	There may be more opportunities to adopt some of the ITIL definitions, beyond the Incident Management and Configuration Change Management topics noted below.

CIP 002-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
Attachment I, Medium Impact Rating (M)	2	Stacy Bresler NESCO	This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cybersecurity controls. The wording of this measurement has had much debate over the last several months and there isconflicting understanding on what this actually entails. Based on the latest information, the SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered.
Attachment 1	2	Carol Muehrcke Adventium	Text before 2.1, 2.2 does not read correctly in connection to those items. We are unsure how it should be corrected.
Attachment 1	2	Scott Hughes, Marc Child (GRE)	Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Criteria 2.11 contains the words “…if destroyed, degraded, misused”. (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the “15 minutes” qualification as defined at the top of the Medium Impact Rating section. Criteria 2.12 refers to a “system” – as in “Each system or Facility…” –

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. The SDT may want to consider removing “Each system or”. Page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. This graphically illustrates the overall intent of the SDT for CIP-002-5. However, when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn’t any appreciable difference between High and Medium requirements. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be “All these assets have a Critical Impact Rating”. Requirement 1 would therefore be “For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011”. If there are cases (like CIP-010-5-R3.2) where specific “High Impact” systems are intended, then the SDT could consider stating so in the requirement; “For Control Centers, perform an active vulnerability assessment every 39 months…”.
Attachment1	2	Stacy Bresler NESCO	Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			20 minutes? The term "adversely impact" is not clearly defined. A concern with the 15-minute time limit is that it is really related to the ability to make generation with the contingency reserve available within 10 minutes of a disturbance and then allow the Transmission Operator/Balancing Authority to restore firm load within 15 minutes of a disturbance. The methodolgy does not equate on the security side. The security side is that you are attempting to reduce the risk that you have to recover within 15 minutes. A possible approach is to prescribe protective measures by facility type, system type, and device type. Attachment 1 is a good start, but it could be rewritten to be specifically based on preventing the need to restore. Suggest changing wording “would, within 15 minutes, adversely impact” to “could adversely impact.” There is a significant difference between would and could. A more specific definition of “adversely impact” would be useful, but it is unclear whether this is practical given the number of BES reliability operating services and the utility circumstances.
R1	3	Carol Muehrcke Adventium Scott Hughes, Marc Child	Clarify – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for v5, a bit more explanation would be useful. What constitutes a “change to BES Elements…” per part 1.1? The SDT may want to consider modifying this language to simply state that new or retired assets be added or removed from the list within 30 days

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		(GRE)	of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems. Therefore, the SDT may want to consider modifying the last sentence to "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls". (New words are "is not required, but").
R2	4	Scott Hughes, Marc Child (GRE)	The SDT may want to consider that this requirement and all others that use the words "…initially upon the effective date of the standard…" have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It's not reasonable to assume that every entity is capable of executing all procedures "upon the effective date". Minor point, but this is the first time "CIP Senior Manager" is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section "B. Compliance", under sub-section "1.2 Evidence Retention", there is a typo in the second to last line. Please change "complaint" to "compliant".
Attachment 1	2	Mladen Kezunovic, Tomo Popovic (TLI)	Phasor Measurement Units: There is still a debate whether PMUs should be considered high impact assets. There is a trend of pushing PMUs to be considered as low-impact assets. This generally depends on PMU use case scenario.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			Since these devices provide relatively high speed measurements, there are several use scenarios where these measurements can be used in closed loops, or by operators for control. Assuming PMU use for control, they could easily be considered as high impact assets since power system operators may depend on their use. In some other scenarios, where PMUs would be used only for monitoring and maybe as additional information sources to increase redundancy of measurements, they could be consideredas low-impact assets similarly to digital fault recorders. NERC could consider providing guidance on this issue. This comment would need revision, since the term critical asset is no longer in the standard. Medium and High impact are defined in CIP 002, specifically in the Attachment 1. Medium and high are defined in terms of “BES reliability operating services,” which explicitly include monitoring and situation awareness per the Guidelines and Technical Basis section in CIP 002-5. Hence if this comment still applies, it would be good if it explained why attachment 1 is unclear in terms of classifying PMUs as med or high impact in a specific case. (I am unable to judge this.) If this comment still applies, I agree it would be against CIP 002-5, Attachment 1, which is NERC question 2. I am in email exchange with Mladen about this and the relay comment above. Tomo Popovic: Moved here as suggested by Carol Muehrcke above. Deleted from the general part, terminology adjusted briefly.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
Attachment 1	2	Mladen Kezunovic, Tomo Popovic (TLI)	Multifunctional devices as high impact assets: Handling of multifunctional devices identified as high impact assets, for example, protection relays may be addressed through sets of restrictive non-functional requirements. Besides of its protection function, digital protective relays typically provide monitoring and reporting functions. CIP may be too restrictive or lacking guidance on how to approach accessing the protective devices and other multifunctional devices to allow for data and report retrieval. This is considered a significant problem by power utilities and currently they are restricted on how to retrieve and use recorded data and reports remotely.

CIP 003-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R2	7	Stacy Bresler NESCO	The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training and Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography. The list of

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Annabelle Lee (EPRI)	topics does not include such items as: access control, training and awareness, audit and accountability, I&A, planning, risk management, information system and information integrity, continuity of operations, information system development and maintenance. Please consider looking at the full list of families included in NISTIR 7628 and consider augmenting the topics list. As stated, "BES Cyber Systems." This does not include BES cyber assets or facilities. Please clarify.
R4	9	Chan Park N-Dimension Solutions	This rule states "...individuals who have access to BES Cyber Systems..." This could be emphasized to state that the "access to BES Cyber Systems" means logical and/or physical access. Even techs without cyber access to equipment in substations, for instance, should nevertheless be aware of the cyber security policies governing that equipment, such as, for example, no use of thumb drives.
Application guidelines for R2	7	Andrew Wright & Dan Widger, N-Dimension Solutions	There are a number of technical issues raised here that, in some cases, can be technically enforced, and not just required by policy. Consider moving and/or adding these to other CIPs where they are more appropriate. Also many of these issues go beyond the scope of the standards and are not required for compliance. This may cause confusion as to what is required for compliance. • Organization stance on use of wireless networks (*this would be optimally addressed in CIP005)* • Monitoring and logging of ingress and egress at Electronic Access Points *(this is in CIP007 R4.1.1)*

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			• Maintaining up-to-date anti-malware software before initiating interactive remote access *(is in CIP007 R3.4)* • Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access (*this would be optimally addressed in CIP007 R2.x)* • Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating interactive remote access (*this would be optimally addressed in CIP005)* • For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's interactive remote access controls (*this would be optimally addressed in CIP011 R1.x)* • Monitoring and logging of physical ingress and egress (*this would be optimally addressed in CIP006 R1.x, noting that egress logging / monitoring in not in the current CIP standards)* • Availability of spare components (*this was in CIP v1-v4, but doesn't appear to be in CIP v5*) • Break- fix processes (*this would be optimally addressed in CIP010 R1.x)*
R4	10	Scott Hughes, Marc Child (GRE)	Are the measures listed under M5 meant to be prescriptive? These are very specific and imply requirements. Throughout the standards, measurements are now tightly tied to requirements and are much more prominent. However, examples should be stated as examples, so that "measures" do not become "requirements" . The SDT may want to consider stating (somewhere)

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.

CIP 004-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
1.1	13	Chan Park N-Dimension Solutions	If awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks. This malware might then be used to stage attacks against electronic security perimeters protecting BES cyber systems. The Rationale for R1 indicates that personnel who have authorized electronic access and/or authorized unescorted physical access to

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Stacy Bresler Annabelle Lee (EPRI)	BES Cyber Systems are to maintain awareness of best security practices. Neither the R1 requirement language nor the R1.1 table requirement make mention of best security practices rather the requirement states security concepts. Also, It would seem that if the expectation is for those personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to be the recipients of such awareness then the requirement should be explicit in that regard. It was noted that the Change Rationale for R1.1 states "Changed to remove the need to ensure everyone with authorized access receives this awareness" which appears to be counter to the Rationale of R1. Responsible Entities does not appear to include operators, specifically, those who operate the BES cyber system and/or BEST cyber assets. Operators should also receive training.
	14	Scott Hughes, Marc Child (GRE)	Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please consider rewriting to make this clearer. For example, 2.2 could be reworded to add the clause “including electronic access controls” OR 2.4 could be reworded to say “The training required under 2.2 shall include training on electronic access controls.”
R3	15	Annabelle Lee (EPRI) Scott Hughes,	Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for “transient” workers. By

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Marc Child (GRE)	transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
4.1	16	Chan Park N-Dimension Solutions	Without requiring verification of credentials, e.g., government issued photo ID, how is the utility able to trust an employee's identity?
4.2	16	Chan Park and Andrew Wright, N-Dimension Solutions	The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements.
4.2	16	Chan Park N-Dimension Solutions	The criminal check record is private confidential information and, therefore, needs to be stored securely.
4.4	16	Chan Park & Andrew Wright, N-	It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Dimension Solutions	utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
R5	17	Scott Hughes, Marc Child (GRE)	One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different and it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R7	19	Stacy Bresler NESCO	Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. The SDT may want to reconsider this requirement. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
R6	18	Scott Hughes, Marc Child (GRE)	Parts 6.1, 6.2, and 6.3 state that “access permissions shall be the minimum necessary…” This appears to be a goal and the SDT may want to consider moving this sentence to the Rationale or Guidelines section. Part 6.3 should include a cross-reference to CIP-011-1-R1.2, as in “…as documented in the entities information protection access control procedures in CIP-011-1-R1.2.” Parts 6.1, 6.2, and 6.3 include the qualifier “…except for CIP Exceptional Circumstances”. For consistency, this language could

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access to control systems as well as cyber access. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per an earlier comment, the "minimum necessary" language throughout R6 may be difficult for entities to prove and the SDT should consider moving it to the Rationale or Guidelines section.
	20	Scott Hughes, Marc Child (GRE)	In the Guidelines section of CIP-004-5, the last sentence under Requirement R3 (and again under R4) states "…by the single senior management official identified in Requirement R1". This should be re-written to say "…by the CIP Senior Manager or delegate identified in CIP-003-5-R1". In the Requirement R4 section of the Guidelines, the reference to CIP-011 is a typo and should state CIP-004. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph could be modified to state "Best practice recommends that access authorization and provisioning should not be performed by the same individual". Some entities are too small for strict separation of duties to be feasible.

CIP 005-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
none	21	Andrew Wright, N-Dimension Solutions	There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have the integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP.
A 4.2.4.2 Introduction to every CIP	21	Andrew Wright, N-Dimension Solutions	Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.).
R1	21	Andrew Wright, N-	A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1, R1.2,

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Dimension Solutions	R1.3, and R1.5 all provide exclusions for non-routable protocols. Of these, R1.5 is the only requirement for which there might be limited choices of technical solutions currently available on the market. There are also exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims.
R1	21	Andrew Wright, N-Dimension Solutions	This requirement should also apply to Associated Electronic Access Control Systems and perhaps also Associated Protected Cyber Assets, since where authentication servers are used separately from the EAP devices, they need to be at least as strongly secured as the EAP devices themselves.
R1.5	21	Stacy Bresler NESCO	This requirements states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There are no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity."
	21	Scott Hughes, Marc Child (GRE)	How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please consider qualifying "outbound" to be "…inbound and, where implemented by the entity, outbound access permissions". In Part 1.5, the term "malicious communications" is too vague. The SDT could consider changing 1.5 to say "A documented method for malicious traffic inspection at each EAP". The third paragraph states "This requirement applies only to communications for which 'deny by default' type requirements can by universally applied…". This sort of language, while useful, should more properly be included in the requirements. The SDT could consider making clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used. As stated, "A documented method for detecting malicious communications at each EAP." Does this include both inbound and outbound communications? Malicious communications can also be sent from the BES through the EAP.
2	22	Andrew Wright, N-Dimension Solutions	This requirement should also apply to Associated Electronic Access Control Systems and perhaps also Associated Protected Cyber Assets, since where authentication servers are used separately from the EAP devices, they need to be at least as strongly secured as the EAP devices themselves.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
2.2	22	Chan Park and Andrew Wright, N-Dimension Solutions	As stated, “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.” However, this statement does not address end-to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. Connections between initiating Cyber Asset and Intermediate Device can be encrypted most times using 3rd party applications, however the connections between the Intermediate Device and Remote gateway or end device (IED) is often not technically feasible. It does not state anything about "Authenticating based on certificates”. There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure may need to further assessment.
		Annabelle Lee (EPRI)	As stated, "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Please consider replacing "encryption" with cryptographic techniques. Cryptographic techniques includes

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			encryption, integrity, and non-repudiation. As stated, "Require multi-factor authentication for all Interactive Remote Access sessions." Why would multi-factor authentication be required for device to device remote access? As technology evolves, there could be more interactive device to device remote access sessions.
2.3	22	Chan Park N-Dimension Solutions	There is a discrepancy on the usage of multi-factor authentication. In this rule, it states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets “REQUIRES” multi-factor authentication. However, in CIP-007 R5.1, it states to “validate credentials before granting electronic access to each BES Cyber System” which does not state the need for multi-factor authentication. A reference for the definition for strong (two-factor) authentication in the RSA information security glossary at http://www.rsa.com/glossary/default.asp?id=1080
2.3	22	Andrew Wright N-Dimension Solutions	Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006, but while the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number", which is far weaker than the generally acknowledged concept. Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. NERC could consider that the different factors involved in a multi-factor authentication be drawn from

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			at least two different classes of authenticator, the classes being something you know (e.g., password, userid), something you have (e.g., badge, smartphone, token, physical key), or something about you (e.g., fingerprint, retina scan, voice print). Also some requirement for liveness should be included to prevent, for example, a physical key (as in a metal thing with notches) acting as one factor being left permanently installed/attached to a reader.
R1 guidelines	21	Andrew Wright N-Dimension Solutions	Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple google search. Caller-id spoofing services make reliance on caller-id tags questionable. Remote enable or powerup leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone. Problems with dialup modems and methods of securing them are discussed in some detail in"Securing Control Systems Modems" from Idaho National Lab: www.inl.gov/technicalpublications/Documents/3874574.pdf Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections.
		Stacy Bressler (NESCO)	

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			This sentence is unclear: "Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust." Does that mean networks of lesser trust to public networks and, if so, what are those networks? Or is this saying that one should not place low impact BES Cyber Systems on public networks or networks of lesser trust to a corporate network or a network behind an EAP?
none	21	Andrew Wright and Dan Widger, N-Dimension Solutions	It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level.
R2.1	22	Andrew Wright and Dan Widger, N-Dimension Solutions	Use of Intermediate Devices is a good method to reduce the possibility of malware spreading into BES cyber assets. However, simply requiring use of an intermediate device without placing any requirements on that device may reduce security. NERC could consider that: 1. Intermediate devices must be within a secure subnet implemented by the entity subject to the same change control methodology as other Cyber Assets subject to CIP, that forces all inbound and outbound traffic to the intermediate device 2. Intermediate devices must log all traffic 3. Intermediate devices must authenticate identity of originator

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			4. Intermediate devices must deploy methods to identify malicious communications and/or block malware.

CIP 006-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
	24?	Chan Park N-Dimension Solutions	This CIP standard no longer has a statement related to “All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter.”
R1	24	Josh Axelrod AlertEnterprise Stacy Bresler	The language could guide physical security measures through a description of acceptable construction materials, construction practices, and based on facility type. Specification on vegetation management, lighting requirements, stand off distances, periodic patrol, etc., should be included. The key point is that we are drafting physical security standards for the electric industry. It is important to write down a "standard" that people know how to follow for the sake of consistency and achieving the goal of protecting the BES Cyber Assets and BES Cyber Systems. For example, tell them they need an 8ft tall mesh fence with shakers and motion detection if that is needed to establish physical security

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Annabelle Lee (EPRI)	perimeter. This is also necessary to help in making this requirement auditable. Without more description and additional security control specific the plans generated by the responsible entities may only identify the minimum stated requirement which can leave gapping holes. ASIS physical security standards could be considered as one source of generally accepted good practices that could be leveraged to help make CIP-006-5 a more robust and adequate security standard. As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. As stated, "Utilize two or more different and complementary physical access controls to..." Examples are provided – but they are not mandatory. What if the associated protected cyber asset is a laptop? Requirement 1.6 references only systems. Early CIPs also reference assets and facilities.
		Scott Hughes, Marc Child (GRE)	How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? The SDT may want to consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets.
R1.2 / R1.3	24	Stacy Bresler NESCO	The requirement statements in R1.2 and R1.3 address ingress controls; however, the associated measures state egress and ingress.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			If egress controls are an expectation then the requirement should make it clear as to what the responsible entity is required to do.
R2	25	Josh Axelrod AlertEnterprise	Continuous monitoring should be defined with a maximum time frame of escort, communication mechanisms, minimum communications capability during escort, required periodic communications, maximum distance between escort and visitor, visitor identification mechanisms, escort qualifications.
R3	26	Josh Axelrod AlertEnterprise Annabelle Lee (EPRI)	Testing could be at least daily operational checks by security staff using the equipment. This can be simple camera pans, alarm testing, etc. Physical maintenance could be performed based on the environment, e.g., Gen plants are dirty so the condition may warrant a high frequency of checks due to carbon and dust build up, control centers are typically well enclosed, so lower frequencies are needed. NERC could consider adding a requirement to retest if the system fails.
R1.5	24	Andrew Wright and Dan Widger, N-Dimension Solutions	The control as documented is to issue alerts for un-authorized physical access, however there is no control to document results of followup. We propose that events (from alerts) and findings are documented, or even that a summary of findings per period (daily / weekly, etc) are documented. For consideration: “Issue real-time / immediate alerts in response to unauthorized physical access attempts, and investigate and respond to **alerts** before the end of the next calendar day, and document

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			outcome.”

CIP 007-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R1	28	Andrew Wright & Dan Widger, N-Dimension Solutions Scott Hughes, Marc Child (GRE) Art Conklin(UH)	Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. For Part 1.1, SDT could consider acknowledging the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. ". . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement".
	29	Scott Hughes, Marc Child (GRE)	The SDT may want to consider revising Part 2.2 to say "Identify applicable security-related patches or security-related updates…" As written, a person could interpret "updates" to mean security-related or not. The words "…that addresses the vulnerabilities within a defined timeframe" could be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say "Execute the remediation plan documented in Part 2.2"?
R2	29	Annabelle Lee (EPRI)	Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			As stated, "A process for remediation, including any exceptions for CIP Exceptional Circumstances." This is vague – and could be more specific. Also, this should be linked to configuration management requirements and incident response requirements, as applicable.
R2.1	29	Stacy Bresler NESCO	This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations.
	30	Annabelle Lee (EPRI)	As stated, "Deploy method(s) to deter, detect, or prevent malicious code." This does not address remediation if the malicious code impacts a BES system. How does this requirement specifically relate to separate boundary protections? This requirement appears to be mandatory for every system, rather than to different systems at the boundary. As such, the requirement drives a specific architecture. At what level of the system is this required? Does this include the boot code/kernel, the OS, the applications, etc.? How does this apply to embedded systems? As stated, "Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection.
R3.3	30	Stacy Bresler NESCO	30 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk.
R3.4	30	Stacy Bresler NESCO	There does not appear to be any consideration for the possibility of the introduction of malicious code through a cyber asset or network-media device connected to the same network (within an ESP or behind the same EAP) as a BES Cyber Asset or BES Cyber System. The definition of a Transient Cyber Asset states that it is a: "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System." Consider changing the definition of a Transient Cyber Asset to include assets connecting to the same network where a BES Cyber Asset or BES Cyber System is connected.
R4	31	Andrew Wright, N-Dimension Solutions	A comment in the summary of changes for CIP 005 R1 states that "the non-routable protocol exclusion no longer exists". However, R4.2 and 4.3 provide exclusions for non-routable protocols. We recommend removing these exclusions, as the summary of changes claims.
R4	31	Andrew Wright	There is a requirement to log events (4.1), a requirement to generate

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		& Dan Widger, N-Dimension Solutions	alerts for certain important events (4.2), and a requirement to detect and activate a response to event logging **failures** within one day (4.3). There is no requirement to activate a response to events important enough to raise an **alert** within any time period. Dealing with the actual alerts is at least as important as dealing with logging failure.
		Annabelle Lee (EPRI)	As stated, "4.1.4. Any detected potential malicious activity." How will "a potential malicious activity" be determined? This can be wide open to interpretation as what is “potentially malicious.” Why log every successful logon? NERC could consider logging all events related to privileged accounts. As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? As stated, "(i) dated event logging failures and screen-shots showing how real-time alerts were configured." Configured real-time alerts are not directly related to event logging failures. These are different events. NERC could consider clarifying the requirement or developing two requirements. As stated, "potential event logging failures." Logging failures are typically due to a full log or other basic problem. How is a bi-weekly review going to address this problem? A summarization may miss certain events. As stated, "Activate a response to rectify any deficiency identified

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			from the review before the end of the next calendar day." It is not always possible to rectify a deficiency within a short period of time. This requirement may need to be split into two requirements – one addressing logging failures and a second addressing security incidents.
R4.2	31	Stacy Bresler NESCO Andrew Wright & Dan Widger, N-Dimension Solutions	The Measures and Change Description/Justification indicated that analysis is expected; however the requirement states that necessary alerts need to be established. Consider rewording the requirement to make analysis of the alert a clear objective. There is no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output. If an entity does not have expertise to understand what alerts are possible, and what the alerts may indicate, then the alert generation exercise called out in the Measures is not effective. Furthermore, a utility might simply decide that no alerts need a real-time alert. We recommend that unauthorized access attempts, at a minimum, be considered to require real-time alerts.
R4.5	31	Andrew Wright & Dan Widger,	As written, R4.5 requires log review exactly every two weeks. Since the intent of this rule is to require a review at least every two weeks,

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		N-Dimension Solutions	we recommend adopting wording for this requirement that is similar to what was recommended earlier to fix the definition of the term "annual". Specifically, we recommend something like " an entity is out of compliance with R4.5 unless, within the preceding 14 calendar days, it has reviewed a summarization or sampling of logged events".
	32	Annabelle Lee (EPRI)	As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These could be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. As stated, "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." Consider changing default passwords on devices. Because a default password is unique to a device does not imply that it is secure. As stated, "A process to limit, where technically feasible, the number

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." Consider adding an exception for emergency situations. Also, this is a potential method for launching a denial of service attack. The decision to limit the number of unsuccessful authentication attempts should be based on the potential risk. Consider adding more details in the requirement related to the potential risk.
R5.5	32	Andrew Wright N-Dimension Solutions Scott Hughes,	Long passwords are primarily required to defend against offline password attacks. Increasing the minimum password length from 6 to 8 characters is not adequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. All possible 6-character passwords can be tested on a supercomputer such as the Tianhe-1A in approximately 1 second, or on a distributed EC2 cluster in approximately 15 seconds at a cost of 50 cents. Raising the minimum length from 6 to 8 characters only requires an attacker to spend 96*96 times longer to try all passwords, which is still less than a day using cloud-based distributed computing. Furthermore, on Windows systems that store LM hashes, any password of any length is easily cracked in minutes on a conventional CPU. This applies to all Window systems prior to Windows Server 2008 and Windows 7. We recommend that NERC consider increasing the minimum password length to no fewer than 12 characters on Windows systems and no fewer than 10 characters on Unix-based systems that use

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Marc Child (GRE)	SHA-512, salt, and key stretching. We recommend that NERC consider disabling LM hashes on all Windows servers, clients, and domain controllers. Third, we recommend that NERC consider guidance accompanying the CIPs that point out that using long passwords, even those that satisfy the complexity metrics of 5.5.2, does not automatically result in strong passwords. For a real-world example, The Tech Herald reports that of the 860,160 Stratfor passwords leaked late 2011, they were able to crack roughly 10% of them in a little over 4 hours using a CPU-based (ie. no GPU acceleration) cracking tool. Many of these were longer than 8 characters. See supporting document "NESCO Common TFE Analysis: CIP-007 R5.3 Password Complexity" available as EPRI Tech report XXX **(Not sure how we want to reference this)** Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			may be stricken, and the asset types moved to the Applicability column.

CIP 008-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
1.2	34	Stacy Bresler NESCO	Even though the R1 rationale states that reportable incidents would follow the EOP 4 actions and timelines, the requirement language cow;d be more specific regarding that expectation.
1.3.1	34	Chan Park N-Dimension Solutions	What happens if there is a third-party IT company that handles the utility's cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
R1	34	Elizabeth Sisley, Calm Sunrise Consulting	Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/ General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
	35	Scott Hughes,	Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Marc Child (GRE) Annabelle Lee (EPRI)	MUST be used, yet deviations are allowed. Recommend rewording this requirement to say “When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review”. As stated, "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." Consider making testing cyber security incident plans a separate requirement. Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity.
	35	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #34 above
	36	Scott Hughes, Marc Child	The Change Description field mentions “DHS Controls”. What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, consider including a timeline/graphic in

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		(GRE) Annabelle Lee (EPRI)	the Guidelines section to visually demonstrate the lifecycle of the plan. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc. As stated, "Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan." Consider updating the plan based on new threats and vulnerabilities.
	36	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #34 above
	37	Elizabeth Sisley,	Refer to comments on #34 above

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Calm Sunrise Consulting	

CIP 009-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R1.3	38	Chan Park N-Dimension Solutions	Protection of backup media and backed up information is only lightly mentioned in this rule. Consider adding greater emphasis on the protection of backups, such as off-site storage and other physical protection, so that sensitive information in backup files (network configurations, device configurations, passwords, etc.) is protected.
		Scott Hughes, Marc Child (GRE)	Is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify. For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Annabelle Lee (EPRI)	assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. As stated, "Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts." The definition of roles and responsibilities and the names of specific individuals assuming those roles are two different areas. Roles and responsibilities may not change significantly over time, unless there is a new vulnerability or threat. The identity of individuals may change – based on people moving, terminating, etc. Consider having the list of specific individuals in a separate document.
R3.2	40	Andrew Wright & Dan Widger, N-Dimension Solutions	For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both.
	39	Scott Hughes, Marc Child (GRE)	Consider revising part 2.1 to read “Test the Recovery Plans at least once every calendar year”, and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be “backed up” in a traditional IT sense. As stated, "...initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment." The other components are tested every 15 months – why is this 39 months? This assumes that a utility has a complete representative environment. This may not be realistic for all the BES associated systems. If there is a significant cyber security incident, the plan could be tested once the system is made operational. This will ensure the revised plan is accurate.
	40	Scott Hughes, Marc Child (GRE)	Due to the complexity of the testing and review of the BES Cyber Security incident response plans, NERC could consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Also, not all cyber assets can be “backed up” in a traditional IT sense.
R3.3	40	Glen Chason EPRI	We recommend that the Measures in Part 3.3 of CIP-009-5 Table R3 be updated to include identification and documentation of the date of any event or lesson learned that results in an update to the recovery plan.
R3.4	40	Glen Chason	Table CIP-009-5 R3 parts 3.4 and 3.5 need the sub-headers titled Part Part Part Part updated to Part Applicability Requirements Measures.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		EPRI	
R3.5	40	Glen Chason EPRI Annabelle Lee (EPRI)	NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication. As stated, "or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned." Consider revising the plan after a significant cyber security incident to ensure that it is accurate. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. As stated, "Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change." As discussed earlier, the basic recovery plan should not be linked to specific individuals in an organization. The list of POCs should be kept separate from the plan and updated regularly – based on personnel changes. “Technology changes” is a vague term and could refer to software, hardware, firmware and may or may not be security relevant. Consider clarifying the definition to focus on security relevant changes.

CIP 010-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R1.1	42	Stacy Bresler NESCO	This appears to be an asset inventory and not a true configuration baseline requirement. If a configuration baseline is to be achieved for the sake of assuring that the BES Cyber Asset can be monitored for changes, then this requirement should also include a system level baseline configuration action that can be achieved. Other than security patch level and available network ports, there is no specific requirement to document the security controls. Although, it could be inferred that would be required as part of 1.1.3 and 1.1.4.
		Scott Hughes, Marc Child (GRE)	For Part 1.1.4, the word “scripts” is generic and thereby difficult to address. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify or revise the words “and scripts”.
		Annabelle Lee (EPRI)	As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version)

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
			intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols.
R1.1	42	Chan Park N-Dimension Solutions	The baseline configuration requirements is missing "Network Topology" – "Network Topology" is suggested in NIST SP800-53 CM-2 "Configuration Management" ---> "Baseline Configuration".
R1.1	42	Andrew Wright & Dan Widger, N-Dimension Solutions	NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc.
R1.1	42	Andrew Wright & Dan Widger, N-Dimension Solutions	NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
R1.1	42	Glen Chason EPRI	NERC could consider adding firmware and programmable device load versioning to the list of items in the configuration baseline. This could include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals.
R1	42	Elizabeth Sisley, Calm Sunrise Consulting	Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
R2	43	Carol Muehrcke Adventium	NERC could consider adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes.
R2	43	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above
R3	44	Carol Muehrcke Adventium Scott Hughes,	Vulnerability analysis looks for any weaknesses - it is more than an audit of implementation against design For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Marc Child (GRE)	just aren't economically feasible. What is the acceptable deviation between test and production? For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it may not make sense.
R3	44	Andrew Wright & Dan Widger, N-Dimension Solutions	There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems.
R3.1	44	Andrew Wright & Dan Widger, N-Dimension Solutions	This requirement does not compel an entity to take any action based on the results of the assessment to correct vulnerabilities, and is weaker than the language in R8.4 of CIP-007-3 currently in force.
R3.2	44	Andrew Wright, N-Dimension	R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement.

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Solutions	As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less.
R3	44	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above
	45	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above

CIP 011-5

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
entire	46?	Andrew Wright & Dan Widger, N-Dimension Solutions	This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information.
none	46?	Andrew Wright & Dan Widger, N-Dimension Solutions	Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access.
R1	46	Chan Park N-Dimension Solutions Glen Chason EPRI	The measures column in R1.1 talks about "training materials that ... to recognize BES Cyber Security Information." but does not contain information about having training materials for handling BES Cyber System information. Table CIP-011-1 R1 parts 1.2 and 1.3 need the sub-headers titled Part Part Part Part updated to Part Applicability Requirements Measures.
R2	47	Chan Park N-Dimension Solutions	The statement, "...the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media." does not clearly address secure sanitization of media. It is recommended that NIST SP800-88 is followed by the utilities to safely sanitize the information in the media. Some examples of safe sanitization methods according to NIST SP800-88 are: Clearing information in a media using an overwriting software or

CIP Part/ Section/ Requirement	NERC CIP questionnaire number	Originator	Comment
		Scott Hughes, Marc Child (GRE)	hardware, Purging using degaussing tool for magnetic media, Destroying by shredding, Disintegration, Incineration, Pulverization, and Melting. Also, another reference for clearing and sanitization is: http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t For Part 2.1, please consider adding language that allows for re-use or redeployment within a similar BES Cyber System.