NESCOR/NESCO Comment Submission for the Second Version of the NERC CIP Version 5 Draft Documents

May 2012

Contributor	Organization
Annabelle Lee	EPRI
Andrew Wright	N-Dimension Solutions
Chan Park	N-Dimension Solutions
Dan Widger	N-Dimension Solutions
Stacy Bresler	NESCO
Carol Muehrcke	Adventium Enterprises
Josh Axelrod	Ernst & Young
Glen Chason	EPRI
Elizabeth Sisley	Calm Sunrise Consulting

CIP xxx-5 General

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
implementation plan	49	Jan 2012 revised May 2012	Andrew Wright, N-Dimension	The implementation plan calls for CIPv5 to come into effect July 1, 2015 (which has been moved out 6 months from the version one draft). Given that CIPv5 has already been in the works for more than two years, it is not clear why the effective date is three years in the future.
several	4	Jan 2012 still applies May 2012	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,

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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 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	May 2012 still applies	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/Systems." Why are cyber assets listed in some VSLs and cyber

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				systems listed in others? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a 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.
several	1	Jan 2012 Revised May 2012	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	Origin Date	Author(s)	Comment
Attachment1	2	Jan 2012	Stacy Bresler NESCO	Phrasing around the term "adversely impact" have been addressed in this new draft. However, it still may be helpful to provide some context around the meaning of "adversely impact". It is understood that in may not be practical given the variables one might need to consider.

CIP 003-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
R1		May 2012	Stacy Bresler (NESCO)	This requirement continues to list a series of policies that do not clearly identify what actual components of such security policies categories would be essential to help assure that an expected security state is achieved

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
			Josh Axelrod (Ernst & Young)	and maintained. The policy levels do not provide enough granularity to assure that there is a consistent and common approach to security policies. The standard could be modified to require entities to not only address the topics identified in the version 5 requirement, but to address them in a manner that reflects a clear relationship of policy and underlying process and/or control framework to the types of BES assets being afforded the protection of the Policy.
R2	7	Jan 2012	Stacy Bresler NESCO	The security policies listed in this requirement should be applicable to all assets regardless of impact. Not including physical control policies and security awareness for high and medium impact assets does not match common security practices. It also does not seem to be a practical or sensical approach to dismiss assets not identified as medium or high from

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
			Josh Axelrod (Ernst & Young)	policy categories listed in CIP-003 R1. The standard should be modified to expand Cyber Security Policy to all levels of BES Cyber Systems, requiring the policy enumeration of protective measures afforded to operational assets.
Application guidelines for R2	7	Jan 2012 still applies May 2012	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				CIP007 R4.1.1) 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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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)

CIP 004-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
1.1	13	Jan 2012	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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.
R3	15	Jan 2012 May 2012 still applies	Annabelle Lee (EPRI)	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.
4.2	16	Jan 2012 still applies May 2012	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.

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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.
4.4	16	Jan 2012 still applies May 2012	Chan Park & Andrew Wright, N-Dimension Solutions	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 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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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.
7.4 and 7.5		May 2012	Annabelle Lee	The requirements 7.4 and 7.5 allow time to remove physical and logical access privileges. Requirement 7.1 requires that termination procedures be initiated immediately. 7.4 and 7.5 allow a malicious

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				individual time to initiate an attack.

CIP 005-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
R 1.3		May 2012	Andrew Wright, N-Dimension Solutions	We agree with identifying and documenting a business purpose for all inbound and outbound access from an EAP. However, this requirement should distinguish access through different kinds of perimeters: 1. EAP allows traffic in/out over an encrypted link to/from another EAP owned/operated by the same entity; 2. EAP allows traffic in/out over a private but unencrypted link (eg. MPLS, point-to-point microwave) to/from another EAP owned/operated by the same entity; 3. EAP allows traffic in/out over an encrypted link to/from a system or EAP owned/operated by a different entity;

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				4. EAP allows traffic in/out over a private but unencrypted link to/from a system or EAP owned/operated by a different entity; 5. EAP allows traffic in/out over the public Internet. These cases involve differing degree of risk, with cases 1 and 2 being generally reasonable and justifiable; cases 3 and 4 utilities risky and avoidable with appropriate VPN technology, and case 5 being of far too high a risk to be acceptable, in our opinion, for any business purpose.
none	21	Jan 2012 still applies May 2012	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 their 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-

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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. The lack of commercially available perimeter security solutions for non-routable protocols, pointed out in the Application Guidelines for CIP-005-5, further emphasizes the need for cryptographic protection of serial links. NERC's Consideration of Comments does not address this comment. This comment directly addresses point 86 in FERC 18 CFR Part 40 approving CIP v4, which states "…we support the elimination of the blanket exemption for non-routable

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				connected cyber systems…"
A 4.2.4.2 Introduction to every CIP	21	Jan 2012 still applies May 2012	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies 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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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.). NERC's Consideration of Comments does not address this comment.
R1	21	Jan 2012	Andrew Wright, N-	A comment in the summary of changes for R1 states that "the non-routable protocol

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		revised May 2012	Dimension Solutions	exclusion no longer exists". However, R1.1 and R1.2 all provide exclusions for non-routable protocols. We note that exclusions that existed in draft 1 R1.3 and R1.5 have been removed. There also remain exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims.
R1.5	21	Jan 2012	Stacy Bresler NESCO	Despite the many changes in the language there is still too much ambiguity. "A method" for detecting communications is only also only half of the equation. There should be a method for detecting and addressing or mitigating detected anomalies. Perhaps a better phrasing would be: "Document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity."

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
2.2	22	Jan 2012 May 2012 still applies	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 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.
none	21	Jan 2012 still applies May	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.

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		2012		
R2.1	22	Jan 2012 still applies May 2012	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 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	Origin Date	Author(s)	Comment
R1	24	Jan 2012 May 2012 still applies	Josh Axelrod (Ernst & Young) 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 perimeter. This is also necessary to help in making this requirement auditable. Without more description and additional security control specific the plans

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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.
			Annabelle Lee (EPRI)	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.
R2	25	Jan 2012	Josh Axelrod (Ernst & Young)	Continuous monitoring should be defined with a maximum time frame of escort, communication mechanisms, minimum communications capability during escort, required periodic communications, maximum

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				distance between escort and visitor, visitor identification mechanisms, escort qualifications.
R3	26	Jan 2012 May 2012 still applies	Josh Axelrod (Ernst & Young) 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.

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
R1	28	Jan 2012 revised May 2102	Andrew Wright & Dan Widger, N-Dimension Solutions	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. Since Draft 1, the word “services has been added to the Requirements, but this does not address the point of this comment. 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 mechanisms where no path around them exists enable security functionality to be placed in a

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				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".
R2	29	Jan 2012	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	Origin Date	Author(s)	Comment
R2.1	29	Jan 2012	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	Jan 2012 May 2012 still	Annabelle Lee (EPRI)	As stated, "Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		applies		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	Jan 2012	Stacy Bresler NESCO	Previous draft stated 30 days between updates, this version increased it to 35 days. Again, 35 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. The current requirement statement is long and confusing as well. Consider breaking it up into multiple sentence with clear requirement statements.
R4	31	Jan 2012 May 2012 still	Annabelle Lee (EPRI)	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?

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		applies		
R4.2	31	Jan 2012	Stacy Bresler NESCO	There is still 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.
5.2	32	Jan 2012 May 2012 still	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		applies May 2012	Carol Muehrcke Adventium	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. It is particularly important to identify administrators with privileges to modify the software itself. For example, I was unable to find a requirement in the standard that would discourage combined accounts for both operating and modifying software. CIP mitigations against malicious software currently appear limited to detection methods in CIP 010 - this would strengthen that position and is an auditable special case of least privilege in accordance with NIST 800-53 AC-6 control enhancement 2, which is required in the NIST baseline for moderate and high impact systems. It reads: "The organization requires that users of

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions." For CIP, at a minimum, "modification of software executing on medium or high impact BES systems" could be filled in the square brackets of this NIST requirement.

CIP 008-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
R1	34	Jan 2012	Elizabeth Sisley, Calm Sunrise	Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) -

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		revised May 2012	Consulting	http://www.itil-officialsite.com/ General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
	35	Jan 2012 May 2012 still applies	Annabelle Lee (EPRI)	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	Jan 2012	Elizabeth Sisley, Calm Sunrise	Refer to comments on #34 above

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
		revised May 2012	Consulting	
	36	Jan 2012	Annabelle Lee (EPRI) May 2012 still applies	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,

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	Comment
				audit policies, etc.
	36	Jan 2012 revised May 2012	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #34 above
	37	Jan 2012 revised May 2012	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #34 above

CIP 009-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
R1.3	38	Jan 2012	Chan Park N-Dimension Solutions Annabelle Lee (EPRI) May 2012 still applies	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 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.
R3.2	40	Jan 2012 still applies May 2012	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.

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
R3.4	40	Jan 2012	Glen Chason EPRI Annabelle Lee (EPRI) May 2012 still applies	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, "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.

CIP 010-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
R1.1	42	Jan 2012	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. Being more descriptive would greatly help the entities achieve this requirement.
			Annabelle Lee (EPRI) May 2012 still applies	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
				version); 1.1.3. Any commercially available application software (including version) 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	Jan 2012 still	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
		applies May 2012		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	Jan 2012 still applies May 2012	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.
R1.1	42	Jan 2012 May 2012	Glen Chason EPRI	NERC could consider adding programmable device load versioning to the list of items in the configuration baseline. This should include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals.
R1	42	Jan	Elizabeth Sisley, Calm	Configuration Management could include industry best practices, which are

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
		2012 revised May 2012	Sunrise Consulting	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	Jan 2012 revised May 2012	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above
R3	44	Jan 2012 still applies May 2012	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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
				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.
R3.2	44	Jan 2012 still applies May 2012	Andrew Wright, N-Dimension Solutions	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. 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

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
				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	Jan 2012 revised May 2012	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above
	45	Jan 2012 revised May 2012	Elizabeth Sisley, Calm Sunrise Consulting	Refer to comments on #42 above

CIP 011-5

CIP Part/Section/Requirement	NERC CIP questionnaire number	Origin Date	Author(s)	comment
entire	46?	Jan 2012 still applies May 2012	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?	Jan 2012 still applies May 2012	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.