CIP004 - Personnel and Training

Name Bob Wallace

Entity Ontario Power Generation

Comments		*Responses*
General	OPG feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. OPG feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	Moved to Requirements section
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	Moved to Requirements section
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Grandfathering is not allowed (see FAQ’s). This sets a baseline.
004-C2,4		

CIP004 - Personnel and Training

Name	Carol L. Krysevig
Entity	Allegheny Energy Supply Company

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.4 - Reference to COMPANY PERSONNEL is confusing and should be clarified. Appears to imply that only employees need to have a personnel risk assessment while the implication of the standard is that all personnel (employee, contractor, vendor) who have unescorted access to critical cyber assets must have a personnel risk assessment completed	Corrected in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Don Miller / Ray Morella

Entity FirstEnergy Corp

Comments		*Responses*
General		
004-R1		
004-R2		
004-R3	R3 - Under Records retention the "background screening" should be changed to "personnel risk assessment".	Accepted
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name	Edwin C. Goff III	
Entity	Progress Energy	
Comments		***Responses***
General	I do not recommend we specify the elements of a BI in the standard, rather let each entity determine what elements will be checked based on the risk. The criminal history check should cover a 5 year period. This is consistent with the length of time covered by the update requirements and will ensure no gaps once the initial BI is complete.	Agreed in principle.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.1 - Clarification requested - In maintaining list of authorized personnel, is it required to list personnel that have "READ ONLY" access rights? Would this apply to IED's located in critical asset substations? M4.4 - Clarification requested - Standard states that Entity shall conduct personnel risk assessment process for all personnel "prior" to being granted authorized access to Critical Cyber Assets... How do you handle existing employees running the system which have not had assessments in last 7 years? Suggest amending to state "...for newly hired employees or for transferring employees which require access to Critical Cyber Assets." M4.4 - For identity verification and background checks, does this apply to 3rd party vendor support personnel when granting access or can this be handled through contractual wording with the vendor that they perform these verifications?	See FAQ#7 for this Standard.
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1	COMPLIANCE section 2.1.2 - Clarification requested - Statement "access control list not updated within 24 hours..." Is this referring to actual revoking of the electronic access right or does this include the paperwork must be updated as well? Removal from access control list for external physical and external cyber access within 24 hours is feasible. Removal from all internal access control lists, all accounts on all assets within 24 hours, is not feasible.	Refers to the list itself.
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Francis J. Flynn, Jr., PE

Entity National Grid USA

Comments		***Responses***
General	National Grid feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. National Grid feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard. National Grid believes that the Levels of Non-Compliance within this standard appars to penalize very large corporations more, where the possibility of the number of instances that personnel might be terminated where they do not meet the turnaround time on control list updates , etc. would not be met. An example of this is if you have 5 errors in an organization that has a list of 10,000 people vs 5 errors where there is a list of 50 people, are these instances both treated equally? Please clarify this point.	N/A…
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	All measures substantially revised to match Requirements.
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.	All measures substantially revised to match Requirements..

CIP004 - Personnel and Training

	Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Now referenced in the Purpose section.
004-C2,4		

CIP004 - Personnel and Training

Name Gary Campbell

Entity MAIN

Comments ***Responses***

General Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.
The way the measures are written, as an auditor I do not care what the requirements tell me should be in a procedure, policy etc. The measures are telling what to look for by the usage of "shall" and then specify what is to be looked for.

Levels of Compliance

Specifiy review times in the requirements and then measure

There are measures that are written but have no levels of non-compliance sush as M6. Please review all measures.

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

CIP004 - Personnel and Training

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Gerald Rheault

Entity Manitoba Hydro

Comments		*Responses*
General	In compliance section 2 focus should be on removing the actual access for personnel rather than updating the list within the prescribe time period.	
004-R1		
004-R2		
004-R3	In CIP-004 R3 "background screening" should be changed to "personnel risk assessment". A similar change is required in M4.6 and D1.4.1.	Changed in Draft 3
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	CIP-004 M4.4 mandates a seven year criminal check prior to granting access. This is not allowed by some hiring regulations. The requirement should be that each company has a policy for personnel risk assessment, and that they can demonstrate following that policy - no additional prescriptive requirements should be presented in this area. The company's policy should cover how contractors (or vendors) with authorized access are treated, but should not prescribe how a company needs to treat such circumstances. Any additional information could be included in the FAQs or reference material. Delete CIP-004 M4.5 as this a Responsible Entity issue and not a NERC issue.	Changed to 5-years in Draft 3 and required for consistency and auditability
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		

CIP004 - Personnel and Training

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Gordon Pietsch

Entity Great River Energy

	Comments	*Responses*
General		
004-R1		
004-R2	Suggest a wording change in Section 2.1.2 Levels od non-compliance to focus on whether the access was revoked within 24 hours (rather than focus on whether the access list was updated).	Changed in Draft 3
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name	Greg Mason	
Entity	Dynegy Generation	
Comments		***Responses***
General	Requirements R1-R4 and Measures M1-M4 ignore the current industry trend to outsource certain functions such as IT support to third parties at remote locations. These Requirements and Measures are not practical to implement in this type of business environment.Also,as stated in the recent NERC Cyber webcast,if you are not applying these types of Requirements and Measures to third party telcom providers(who have the ability to impact Critical Asset operation),it would be inconsistent to apply these Requirements and Measures to providers of outsourced IT support.We request that either this Standard be modified or a FAQ be developed to exempt providers of outsoured IT support from these Requirements and Measures.	Not accepted – such measures can be applied contracturaly to out-source provi
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		

CIP004 - Personnel and Training

004-C2,4

CIP004 - Personnel and Training

Name Guy Zito

Entity NPCC CP9

Comments		*Responses*
General	CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. NPCC Participating Members feel this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	Modified in Draft 3
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	Modified in Draft 3
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	Modified in Draft 3
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Modified in Draft 3
004-C2,4		

CIP004 - Personnel and Training

Name	James W. Sample
Entity	California ISO

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	M2.4 – this is a new requirement and there is no matching requirement in this standard.	Modified in Draft 3
004-M3		
004-M4	M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003. M4.6 – this should refer to risk assessment as in R4 rather than screenings.	Changed in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	2.3.1 – Please include a matching requirement or delete this paragraph.	Changed in Draft 3
004-C2,4		

CIP004 - Personnel and Training

Name Jerry Freese

Entity American Electric Power

Comments		*Responses*
General	The "titles" are inconsistent - either all requirements in the NERC CIP seriees should have titles, or none should have titles. We believe that all requirements should have titles.	Revisions made.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2	Compliance 1.2 - the data should only be stored for 2 years. Storing the data for an extra year makes an even greater burden.	Agreed.
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name	Jerry Heeren	
Entity	MEAG Power	
Comments		***Responses***
General	We suggest that the phrase “background screening” in R3 be replaced by the phrase “identity verification” -- as in other areas of the document.	Agreed.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Jerry Litteer

Entity INL

Comments		***Responses***
General	Does not say security training is tied to employment but infers access to critical cyber assets. Access to critical cyber assets could be a condition of employment. I realize this standard does not want to be prescriptive, but without strong senior management involvement and conditions to employment -- security programs fail. . No mention of what the operator or system administrator training for a suspected incident or trained for expected utilization of the systems and performance indicators.	
004-R1		
004-R2	R2. Training Add the following: R2-a. Additional training should be given as access level increases. R2-b. All training must include vendors, contractor personnel and others who (for example local backup entities) that have access to the data/system. R2-c. Training needs to be updated yearly at a minimum or whenever new requirements / access status dictates.	Too prescriptive for a broad-based standard
004-R3		
004-R4		
004-M1		
004-M2		
004-M3	M4.3 changes to 24 hours terminated with cause and 7 days for change in status -- still too long	Based upon prior comments and practical business applications
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP004 - Personnel and Training

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Jim Hansen

Entity Seattle City Light

Comments		*Responses*
General	Throughout this section the term ‘authorized access’ is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions.	See FAQ#4 for this Standard.
004-R1	R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content.	This is left to the discretion of the Responsible Entity.
004-R2		
004-R3		
004-R4	R4 and M4.4: Both contain the phrase 'prior to'. Please clarify how existing staff should be handled. We specifically do not want to prohibit existing staff from having access while we are performing the required assessments.	The Standards do not apply until after the assessment has been completed.
004-M1	R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content.	
004-M2		
004-M3		
004-M4	R4 and M4.4: Both contain the phrase 'prior to'. Please clarify how existing staff should be handled. We specifically do not want to prohibit existing staff from having access while we are performing the required assessments.	
004-C1,1		

CIP004 - Personnel and Training

004-C1,2

004-C1,3

004-C1,4

004-C2,1 R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content.

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Jim Hiebert	
Entity	California ISO	
Comments		***Responses***
General	Throughout this section the term 'authorized access' is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content.	
004-R1		
004-R2		
004-R3		
004-R4	R4 and M4.4: Both contain the phrase 'prior to'. Please clarify how existing staff should be handled. We specifically do not want to prohibit existing staff from having access while we are performing the required assessments.	
004-M1		
004-M2		
004-M3		
004-M4	M4.6 -- Instead of reading, 'The Responsible Entity shall conduct update screenings at least every five years or for cause', should read, 'The Responsible Entity shall conduct personnel updates as per their documented company personnel risk assessment process at least every fives years or for cause'.	
004-C1,1		
004-C1,2		
004-C1,3		

CIP004 - Personnel and Training

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Joe Weiss

Entity KEMA

Comments		*Responses*
General	This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment	
004-R1	R1. The Responsible Entity shall develop, maintain, and document its Critical Assets security awareness program. Typical security awareness programs do not address Critical Assets.	To be taken into consideration for development of programs under this standar
004-R2	R2. The Responsible Entity shall develop and maintain a company Critical Asset specific cyber security training program... Typical cyber security training programs do not address Critical Assets.	To be taken into consideration for development of programs under this standar
004-R3		
004-R4		
004-M1	M1. The Responsible Entity shall develop and maintain Critical Asset awareness programs designed to maintain and promote sound Critical Asset security practices…. Typical security awareness programs do not address Critical Assets.	To be taken into consideration for development of programs under this standar
004-M2	M2. The Responsible Entity shall develop and maintain a company Critical Asset specific cyber security training program... Typical cyber security training programs do not address Critical Assets. M2.1 The Critical Assets cyber security policy. Typical cyber security policies do not address Critical Assets.	To be taken into consideration for development of programs under this standar
004-M3		
004-M4	M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all company, vendors, and contractors being granted authorized access ... It is not clear that vendors and contractors are addressed and need to be.	N/A
004-C1,1		
004-C1,2		
004-C1,3		

CIP004 - Personnel and Training

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	John Lim
Entity	Con Edison

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	Measure M4.4 currently states: "The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized access to Critical Cyber Assets in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. A minimum of identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check is required. Entities may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position." The operating requirements and environments of Responsible Entities vary widely. Prescribed requirements may not be appropriate depending on these requirements and environments. In addition, the background check requirement should not be contingent on any “bargaining agreement” . It is our opinion that this type of requirement is similar to a local law and the law overrides. Proposed M4.4: "The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized access to Critical Cyber Assets in accordance with federal, state, provincial, and local laws. Based on this risk assessment, the Responsible Entity will identify personnel which warrant further assessment, which must include a minimum of identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal	Modified in Draft 3

check. Entities may conduct more detailed reviews, as permitted by law, depending upon thecriticality of the position."

Measure M4.6 currently states:

"The Responsible Entity shall conduct update screenings at least every five years or for cause."

Con Edison feels that the Responsible Entity's risk assessment process should determine update screenings.

Proposed M4.6:

"The Responsible Entity shall conduct update screenings as determined by its documented personnel risk assessment process or for cause."

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Karl Tammer
Entity	ISO/RTO Council

Comments		*Responses*
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	M2.4 -- this is a new requirement and there is no matching requirement in this standard.	
004-M3		
004-M4	M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003 M4.6 -- this should refer to risk assessment as in R4 rather than screenings.	
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	2.3.1 -- Please include a matching requirement or delete this paragraph.	
004-C2,4		

CIP004 - Personnel and Training

Name	Kathleen M. Goodman
Entity	ISO New England Inc.

Comments		***Responses***
General	ISO-NE feels CIP-004 needs more work before it is ready for ballot. ISO-NE feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	N/A
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	M2.4 is a new requirement that should be specified in the corresponding Requirements section.	All measures substantially revised to match Requirements.
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.Measure 4.6 should be modified. The requirement for a regular 5-year update to the security screening is not consistent with Requirement R4, which states that a risk-based approach be used. The need for re-screening should be cause only.	All measures substantially revised to match Requirements.
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures	Now referenced in the Purpose section.
004-C2,4		

CIP004 - Personnel and Training

Name	Keith Fowler
Entity	LG&E Energy Corp.

Comments		***Responses***
General	We are in agreement with the comments submitted by the ECAR CIPP group	
004-R1		
004-R2		
004-R3		
004-R4	B. R4--Recommend: Most contractors and service vendors conduct criminal background checks as required by their contracts. However, due to privacy concerns, contractor companies may not release criminal background information on their employees to utilities. We recommend adding a statement that the "personnel risk assessment" can be based upon the certification of the contractor that their employee's background is "clear". Change To (add): The personnel risk assessment can be based upon the certification of the contractor that their employee's background is clear.	See FAQ#7 for this Standard.
004-M1		
004-M2		
004-M3		
004-M4	C.M4.4 Recommend: Latitude should be provided under "personnel risk assessment process" to substitute a "known" history of an employee for the "seven year criminal check." In essence, "grandfathering" those with a clean 10, 20 or 30 year history with a company in lieu of a seven year check. Criminal histories should then be required for all "company" employees with less than seven years. Change to (add): Employees with a clean 10, 20 or 30 year history with a company may be grandfathered in lieu of a seven year check. A criminal history check is required for all company employees with less than seven years.	No grandfathering accepted – see FAQ#1 to this Standard.
004-C1,1		
004-C1,2		
004-C1,3		

CIP004 - Personnel and Training

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Ken Fell

Entity New York Independent System Operator

Comments		***Responses***
General	This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.	
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	M2.4 has no corresponding requirement, one should be added.	Modified in Draft 3
004-M3		
004-M4	Measures 4.1-3 should be removed as they are redundant with CIP 003. Measure 4.6 should be based on risk assessment process.	Modified in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Non-compliance Level 3 2.3.1 has no corroborating requirement.	Modified in Draft 3
004-C2,4		

CIP004 - Personnel and Training

Name	Kenneth A. Goldsmith	
Entity	Alliant Energy	
Comments		***Responses***
General	Reword Levels of non-compliance 2.1.2, 2.2.2, 2.3.2 … in which the access was not revoked (rather than access control list updated)	An audit cannot be performed unless the list reflects the action taken.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	2.1.4 The concept of "Key Personnel" is unclear. This term is not defined. This is the only place where the term is used	Agreed.
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Kurt Muehlbauer

Entity Exelon Corporation

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4	M4.6 requires update to the personnel risk assessment at least every five years or for cause. Since employees of the responsible entity are under constant observation by management personnel and performance is reviewed on an on-going basis, we believe that it is not necessary to require reassessments for employees of the responsible entity.	5-year requirement retained for consistency and auditability
004-M1		
004-M2	Is the intent of M2 to require that all personnel with access to Critical Cyber Assets be retrained annually on cyber security, or just that the training program needs to be reviewed and updated annually? We recommend that the training program be reviewed and updated annually. We also recommend that since M1 requires quarterly reinforcement of sound security practices, that the responsible entity will be responsible for determining if any retraining is necessary.	Requires annual training and quarterly reinforcement through awareness remin
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		

CIP004 - Personnel and Training

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	L.W. Brown
Entity	Edison Electric Institute

Comments		*Responses*
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.3. To improve the clarity of the language, we suggest changing the third line to read as follows: "…change in status when they are no longer allowed access…" M4.4, 4.6. These two Measures should be clarified to express that they do apply to contractors and vendors.	All measures substantially revised to match Requirements.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Compliance 2.1.2. Since updates need to made to actual access as well as to the access lists, we suggest modifying the second line to read as follows: "…in which access and the access control list were not updated…" Nonetheless, even with such a clarifying change, it is unclear how such a factor will be measured. Against what is such a list to be compared in order to determine whether it was appropriately updated? Compliance 2.1.3. The term "properly" is far too subjective in the context used. How	Not needed due to other clarification.

will an auditor determine what was proper documentation of a personnel risk assessment program, and under what criteria? If not done generally in each of the Definition sections, it would be more useful if this phrase were to be clarified by the addition of language to the effect that interpretations will be acceptable for compliance purposes – even if they may differ from those of other entities or of auditors – as long as they are reasonable or justifiable under normal standards of business decision-making.

Compliance 2.1.5. The phrase “consistently or” should be deleted, as it creates confusion for the auditing process. The intent of the phrase is unclear. Is it consistency of message content or of delivery methodology? The FAQ seems to indicate that variety of methodology is appropriate. In fact, variety of delivery method is one recognized tool for keeping “fresh” a message that needs to be repeated often. Even addressing only message content as opposed to methodology, how would, for instance, posters used in a program at one time be compared to brochures, or emails, or some other method used to raise awareness at another time? It would be far simpler to audit compliance if this item addressed only the frequency of the message delivery.

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Larry Conrad
Entity	Cinergy

Comments		***Responses***
General	FAQ vs. CIP-004-1-- The FAQ's language refers to 'background screenings.' However the CIP-004 language refers to a personnel risk assessment. The FAQ language is no longer consistent with the CIP-004 language. For example, the FAQ's say 'no grandfathering'. Recommend changing the FAQ to reflect current language referring to personnel risk assessments rather than background screenings. Additional Questions: Reference CIP-004-01 Personnel Training, Section M4.4 and the FAQ. How aggressive do the methods need to be in order to address Collective Bargaining Agreements (CBA) to meet the Personnel Risk Assessment, if the CBA does not currently allow? If arrangements still cannot be met through the CBA, will a waiver be granted?	Agreed.
004-R1		
004-R2	R.2.-- "...training program that will be reviewed annually." Language is not clear if the training material or the training of the individuals needs to be reviewed annually or if both need annual review. Modify the language so that the intent is clear.	Agreed.
004-R3		
004-R4	R.4.-- Please provide an explanation of how to deal with background checks on service personnel such as HP used for remote computer support.	See FAQs #2 & #7 for this Standard.
004-M1	M1.-- Awareness: Since annual training is required, a separate awareness program is un-necessary and requirement should be deleted	Awareness is lower-level and for general employee population; training is mor
004-M2		
004-M3		
004-M4	M4.2.-- This measure states: "Review (the list of all personnel and specific access rights) quarterly..." However, CIP-003-1 C. M. 18 states: "...review user access rights...at least annually." See general comment above. Drafting Committee needs to standardize the review/update requirements and provide a consistent table of the frequency for such reviews. C.M4.4-- The language in this section now pertains to a 'personnel risk assessment' rather than a background screening. Therefore, the language "...A minimum of	Substantial revisions made.

CIP004 - Personnel and Training

identify verification (Social Security number verification) and seven year criminal check is required" should be deleted. It is no longer appropriate. Those types of things may not be part of the personnel risk assessment.

C.M4.4-- Recommend that language be inserted stating that bargaining unit employees will be screened prior to granting access to critical cyber assets. If the initial screening proves adequate, subsequent background screening will not be performed on bargaining unit personnel.

M4.6-- Change "...shall conduct update screenings..." to "...shall conduct updated personnel risk assessment..." The intent here is the personnel risk assessment of individuals is updated.

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Larry Conrad

Entity ECAR Critical Infrastructure Protection Panel

Comments		***Responses***
General	Purpose: Recommend changing "screening" to "risk assessment" for continuity of intent throughout the document. Change to: Personnel having authorized access to Critical Cyber Assets, as defined by this standard, are given a higher level of trust, by definition, and are required to have a higher level of risk assessment, training, security awareness...	Agreed.
004-R1		
004-R2	Recommend: Additional wording stating the level of training that personnel receive will be commensurate with their defined roles and responsibilities previously addressed in CIP-003-1, R3. second paragraph. Clarification is needed in the first sentence to specify what needs to be reviewed. Change to: The responsible Entity shall develop and maintain a company specific cyber security training program. The Program and training materials will be reviewed annually. This program will ensure that all personnel having authorized access to Critical Cyber Assets shall be trained annually in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these Critical Cyber Assets. Training will be commensurate with the roles and responsibilities defined in Standard CIO-003-1.	This is left to the discretion of the Responsible Entity.
004-R3	Recommend changing "background screening" to "personnel risk assessment", which is the language used in the rest of the document. Recommend correcting grammar in last part of sentence. Change to: Records -- The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and personnel risk assessment of all personnel having authorized access to Critical Cyber Assets and shall provide records for authorized inspection upon request.	Agreed.
004-R4	Recommend striking the word ...company... to allow flexibility with the assessment processes that contractors and service vendors may apply. Change to: Personnel Risk Assessment -- The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented personnel risk assessment process prior to granting them authorized access to Critical Assets.	Agreed.
004-M1		

CIP004 - Personnel and Training

004-M2		
004-M3		
004-M4	M4.4--Recommend: Delete the last two sentences so as not to impinge upon existing or developing personnel risk assessment policies and processes that companies may utilize. Minor grammar correction in first sentence. Change to: The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to granting authorized access to Critical Cyber assets in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. M4.6--Use "personnel risk assessment" rather than "screenings" for continuity throughout the document. Change to: The Responsible Entity shall conduct update personnel risk assessments at least every five years or for cause.	Agreed in principle.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4	1.4.1 Change to: Document(s) for compliance, training, awareness, and personnel risk assessments; In Additional Compliance Information 1.4.4 - Strike the words ...and annual... . There is no reference to annual security awareness programs within the Requirements and Measures of this standard. Quarterly basis only, is mentioned in M1. Change to: Verification that quarterly security awareness have been conducted;	Agreed.
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Laurent Webber

Entity Western Area Power Administration

	Comments	*Responses*
General	The measures of CIP-004 do not map well to the requirements; in fact the measures add additional requirements. One example is M4.6 which requires updated screenings every 5 years or for cause. This is not part of the requirements and should be eliminated.	Modified in Draft 3
004-R1	R1 and M1: The training requirements in R2 are adequate. As such R1 can be eliminated. R1 and M1: Documenting and maintaining awareness training quarterly and retaining such records for 3 years is overkill. Awareness training is in place at WAPA, but retaining documentation of every employee's attendance, every email, every poster, and other awareness actions is overkill. Measures are important, but there should be a reasonable limit on the documentation requirements. The requirement to retain documentation of awareness training should be eliminated.	3-year retention of auditable proof of compliance is reasonable, considering po
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.2: This measure implies additional requirements for communication and notification between companies that share access to Critical Cyber Assets (substations?). Such communication and notification of personnel actions between companies are not defined elsewhere. If it is the intention of this standard to require inter-company communications to this level, it must be clearly defined in the requirements. M4.3: This measure adds requirements that are not defined in the requirements section. This additional requirement has a cascading effect because many interconnecting-company employees have authorized access to WAPA substations. The communications between interconnecting utilities has been primarily operations-based. This requirement will result in inter-utility administrative and personnel-	Only responsible for documentation for your entity's personnel

based communications at a level never imagined. If this is the desired result it should be clearly stated. Otherwise it must be clearly stated in the requirements section that this applies only to employees of each Responsible Entity.

M4.4: The second sentence includes additional requirements (identity verification and 7 year criminal check) that are not listed in the requirements of this standard. These should be eliminated from the measures, since they are not part of the requirements or the compliance sections.

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Lawrence R Larson, PE
Entity	Midwest Reliability Organization

Comments		***Responses***
General	The Awareness aspect should be eliminated throughout CIP-004, as the additional overhead it requires is not justified for the perceived benefit. The requirements imposed by R2-R4 would do the job adequately without R1 being required. Awareness will normally be done anyway as part of a good program, but defining these specific compliance requirements for this aspect is not sufficiently beneficial to warrant the additional tracking overhead.	Security awareness training is a fundamental part of good security practices an
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.2 requires a mandatory quarterly review of a document. No reviews of any documents on any time-frame shorter than annually should be required in any of these Cyber Security Requirements. M4.4 mandates a seven year criminal check prior to granting access. This is not allowed by some hiring regulations. The requirement should be that each company has a policy for personnel risk assessment, and that they can demonstrate they follow that policy - no additional prescriptive requirements should be presented in this area. The company's policy should cover how contractors (vendors) with authorized access are treated, but should not prescribe how a company needs to treat such circumstances. Standards should focus on WHAT, not HOW. M4.6 should be deleted. Such updated screenings can be provided for if a company feels they are justified. However, in some environments (low turn-over, small groups of employees, etc), such re-screens would be pointless and the overhead and inconvenience would not be justified	

CIP004 - Personnel and Training

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1 We suggest a wording change in Section 2.1.2 Levels of non-compliance to focus on whether the access was revoked within 24 hours (rather than focus on whether the access control list was updated).

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Lee Matuszczak
Entity	U S Bureau of Reclamation

Comments		***Responses***
General		
004-R1		
004-R2	R2. - The second sentence should be revised to delete the reference to personnel "having authorized access to Critical Cyber Assets." All personnel, regardless of access, should be provided training regarding the protection of critical assets.	Not accepted. This language sets the minimum requirement. Responsible entiti
004-R3		
004-R4		
004-M1		
004-M2	M2.3 - Revise to read "The proper control and release of critical cyber asset information." Further, consideration should be given to creating an information protection standard wherein the safeguarding of electronic, stored, written, transcribed, broadcast, and other forms of information is addressed. This would not just include cyber-related information, but information about all critical assets, including personnel.	Too broad for these standards and are a developing area under CEII rules and
004-M3		
004-M4	M4.4 - The second sentence includes additional requirements (identity verification and 7 year criminal check) that may be excessive. Most federal investigations utilize a 5-year criminal check, even for Secret clearance investigations. This requirement should be reconsidered.	
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		

CIP004 - Personnel and Training

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Linda Campbell

Entity FRCC

Comments		*Responses*
General	The Purpose section needs to have the words "as defined by this standard" removed. These words are in reference to the term Critical Cyber Assets; this term will be added to the NERC Glossary upon approval of this standard. Therefore, there is no need to have these words in this standard. In addition the word "screening" should be changed to "risk assessment" for continuity. The second paragraph of the Purpose section should be worded as follows: Personnel having authorized access to Critical Cyber Assets are given a higher level of trust, by definition, and are required to have a higher level of risk assessment, training, security awareness, and record retention of such activity, than personnel not provided access.	Agreed.
004-R1		
004-R2		
004-R3	R3 Uses the term "background screening" this should be change to "personnel risk assessments."	Agreed.
004-R4	R4 states that Personnel be subjected to a personnel risk assessment process. M4.6 uses the term "screenings" rather than risk assessment. The measure and requirements terminology should be consistent. In addition, we believe the "every five years" criteria will be extremely costly and is unnecessary. However, if it remains it should be phased in over a longer time period for implementation than in the current plan. Proposed wording for M4.6. would be: M4.6 The Responsible Entity shall conduct an update of the employee's personnel risk assessment at the following intervals: 1. Seventh year of employment. 2. Fifteenth year of employment 3. Every eighth year after the fifteenth year of employment 4. For cause.	Agreed.
004-M1		
004-M2		

CIP004 - Personnel and Training

004-M3		
004-M4		
004-C1,1		
004-C1,2	The words under Compliance section 1.2. really belong under 1.3. Data Retention. Compliance section 1.2. should be as follows: Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.	Agreed in principle.
004-C1,3	Compliance section 1.3. should be as follows: 1.3. Data Retention 1.3.1. The compliance monitor shall keep audit records for three (3) calendar years. 1.3.2. The Responsible Entity shall keep data for three (3) calendar years. 1.3.3. The Responsible Entity shall keep risk assessment documents for the duration of employee employment. 1.3.4. The Responsible Entity shall keep service vendors records for the duration of their engagement.	Similar revision.
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Lyman Shaffer

Entity Pacific Gas and Electric Company

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.6 Instead of reading, "The Responsible Entity shall conduct update screenings at least every five years or for cause", should read, "The Responsible Entity shall conduct personnel updates as per their documented company personnel risk assessment process at least every fives years or for cause."	Changed in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Marc Butts

Entity Southern Company, Transmission, Operations, Planning and EMS Divisions

	Comments	*Responses*
General	Purpose -- The term access is used but not defined. Is it any type access?	See FAQ#4 for this Standard.
004-R1	In R1-- The term -subject to this standard- is used. One would assume all employees of an applicable Responsible Entity would be subject to the standard but only those with some type of access to a Critical Cyber Access would actually require reinforcement of sound security practices. If the latter group is the case, say so. If the intent is all employees at a responsible entity then say that.	Applicability is dependent in Standard CIP-002, and refers to those with acces
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Under the Levels of Non-Compliance, levels 2.1.3, 2.1.5, and 2.2.5 are too subjective in nature and need to be tightened down to more discrete and auditable measures instead of -not consistently applied- or -not properly documented-.	Language clarified.
004-C2,2	Under the Levels of Non-Compliance, levels 2.1.3, 2.1.5, and 2.2.5 are too subjective in nature and need to be tightened down to more discrete and auditable measures instead of -not consistently applied- or -not properly documented-.	Language clarified.
004-C2,3	Under Level 3 Non-Compliance, move 2.3.3 -A personnel risk assessment program	Agreed

does not exist- to a Level 4 Non-Compliance. It can be argued that most of the risk is from insiders, so doing personnel risk assessments is at least at vital as the other aspects mentioned in Level 4.

004-C2,4

CIP004 - Personnel and Training

Name Patrick Miller

Entity PacifiCorp

Comments		*Responses*
General		
004-R1		
004-R2	For section B, R2, the mandated recipients of information handling training should be clarified. Does this include all janitorial staff? Linemen? Ditch diggers? Electrical contractors and plumbers?	Only includes personnel having “authorized access to critical cyber assets”
004-R3	For section B, R3, it was mentioned in the webcast that the term “background screening” was replaced with “personnel risk assessment.”	Correct
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name	Paul McClay
Entity	Tampa Electric

Comments		***Responses***
General	R4 states that Personnel be subjected to a personnel risk assessment process. M4.6 uses the term "screenings" rather than risk assessment. The measure and requirements terminology should be consistent. In addition, we believe the "every five years" criteria will be extremely costly and is unnecessary. However, if it remains it should be phased in over a longer time period for implementation than in the current plan.	Modified in Draft 3 for consistency
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

CIP004 - Personnel and Training

Name Pete Henderson

Entity Independent Electricity System Operator

Comments		*Responses*
General		
004-R1		
004-R2	In R2, reword the last phrase to read, “and management of sensitive information surrounding these critical cyber assets.”	No longer necessary.
004-R3		
004-R4		
004-M1		
004-M2	M2.4 -- this is a new requirement and there is no matching requirement in this standard.	
004-M3	M3.1 partially duplicates CIP-003 which speaks of requirements to maintain a list of personnel with access to critical cyber assets. Please remove the duplication as it can lead to confusion and duplication of effort.	Agreed – recordkeeping moved to R4 and to Measures and Compliance.
004-M4	M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003. M4.6 -- this should refer to risk assessment as in R4 rather than screenings. The specification of an arbitrary 5 year update is not consistent with the requirement (R4) which states that a risk based approach shall be used.	Agreed.
004-C1,1		
004-C1,2		
004-C1,3	1.3 establishes a new requirement (to retain personnel risk assessment documentation) for the duration of employment. This is inconsistent with 1.2 above. Requirements should not be established in the Compliance section of the standard	Agreed in principle.
004-C1,4		
004-C2,1	The wording of 2.1.5 suggests that reinforcing the awareness program with the minimum quarterly frequency is indicative of level 1 non-compliance. This is inappropriate. The wording requires revision.	Revised.

CIP004 - Personnel and Training

004-C2,2		
004-C2,3	2.3.1 -- Please include a matching requirement or delete this paragraph.	Revised to clarify.
004-C2,4		

CIP004 - Personnel and Training

Name	Philip D. Riley	
Entity	Public Service Commission of South Carolina	
Comments		***Responses***
General	The Public Service Commission of South Carolina believes that both electronic and physical access to critical cyber assets should be withdrawn coincident with notification to the employee of his/her involuntary termination rather than within 24 hours as proposed. The PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.	The expectation is that would generally be done, but the maximum allowable t
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		

CIP004 - Personnel and Training

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Randy Schimka
Entity	San Diego Gas and Electric Co

	Comments	*Responses*
General	CIP-004 refers several times to 'personnel' or 'authorized personnel' when discussing assessments, but doesn't really address how to handle the many vendors and contractors that need access to our critical cyber assets to perform maintenance and other tasks. Please consider providing guidelines for these external but necessary folks. If the term 'personnel' is referring to internal employees as well as external vendors and contractors, we see difficulties in holding external vendor and contractor employees to our own internal standards for background checks and assessments. For example, is the drafting team expecting that we would conduct the same type of background checks on regular employees who work on the EMS and associated systems everyday vs. a Facilities contract electrician that gets access to the critical cyber asset space a few days per year to install new circuits or to perform maintenance? There are probably a dozen different examples of contractors and maintenance workers that visit just once or twice per year to perform maintenance in our critical cyber asset areas where it may be impractical to escort them for 5-8 hours during their work. What suggestions does the drafting team have for handling these types of visitors? Please clarify the term 'authorized access' with respect to electronic or physical access, as there are differences in those types of access that should be handled independently. Please provide examples in CIP-004 or in the FAQ document that outline acceptable examples of Awareness communication.	Included in Draft 3
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		

CIP004 - Personnel and Training

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Raymond A'Brial

Entity Central Hudson Gas & Electric Corporation (CHGE)

Comments ***Responses***

General

CHGE feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

CHGE feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

004-M3

004-M4

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

004-C1,1

004-C1,2

CIP004 - Personnel and Training

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3 Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

004-C2,4

CIP004 - Personnel and Training

Name	Richard Engelbrecht
Entity	Rochester Gas and Electric

Comments		***Responses***
General	NPCC feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. NPCC Participating Members feel this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	N/A…
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	All measures substantially revised to match Requirements.
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	All measures substantially revised to match Requirements
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Now referenced in the Purpose section.
004-C2,4		

CIP004 - Personnel and Training

Name Richard Kafka

Entity Pepco Holdings, Inc. - Affiliates

Comments		*Responses*
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.3. To improve the clarity of the language, we suggest changing the third line to read as follows: "...change in status when they are no longer allowed access..." M4.4, 4.6. These two Measures should be clarified to express that they do apply to contractors and vendors.	Will be changed in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Compliance 2.1.2. Since updates need to made to actual access as well as to the access lists, we suggest modifying the second line to read as follows: "...in which access and the access control list were not updated..." Nonetheless, even with such a clarifying change, it is unclear how such a factor will be measured. Against what is such a list to be compared in order to determine whether it was appropriately updated? The term “properly” in Compliance 2.1.3. is too vague. How will an auditor	Personnel turnover lists compared to access list updates

determined what was “proper”?

The word “consistently” in Compliance 2.1.5. should be deleted, as it creates confusion for the auditing process (e.g. How would posters used in a program at one time be compared to brochures or some other method used to raise awareness at another time?)

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Robert Strauss	
Entity	New York State Electric & Gas Corporation	
Comments		***Responses***
General	NSYEG concurs with NPCC that CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. We believe this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	Quarterly security awareness reinforcement should not be overly burdensome
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	Modified in Draft 3
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	Modified in Draft 3
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Now referenced in the Purpose section.
004-C2,4		

CIP004 - Personnel and Training

Name Roger Champagne

Entity Hydro-Québec TransÉnergie

Comments		***Responses***
General	HQTÉ feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. HQTÉ feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.	N/A
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2	Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.	All measures substantially revised to match Requirements.
004-M3		
004-M4	Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section. Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003. Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.	All measures substantially revised to match Requirements.
004-C1,1		
004-C1,2		

CIP004 - Personnel and Training

004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.	Now referenced in the Purpose section.
004-C2,4		

CIP004 - Personnel and Training

Name Roman Carter

Entity Southern Company Generation

Comments		*Responses*
General	Purpose -- The term access is used but not defined. Is it any type access?	See FAQ#4 for this Standard.
004-R1	In R1-- The term -subject to this standard- is used. One would assume all employees of an applicable Responsible Entity would be subject to the standard but only those with some type of access to a Critical Cyber Access would actually require reinforcement of sound security practices. If the latter group is the case, say so. If the intent is all employees at a responsible entity then say that.	Applicability is dependent in Standard CIP-002, and refers to those with acces
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Under the Levels of Non-Compliance, levels 2.1.3, 2.1.5, and 2.2.5 are too subjective in nature and need to be tightened down to more discrete and auditable measures instead of -not consistently applied- or -not properly documented-.	Language clarified.
004-C2,2	Under the Levels of Non-Compliance, levels 2.1.3, 2.1.5, and 2.2.5 are too subjective in nature and need to be tightened down to more discrete and auditable measures instead of -not consistently applied- or -not properly documented-.	Language clarified.
004-C2,3	Under Level 3 Non-Compliance, move 2.3.3 -A personnel risk assessment program does not exist- to a Level 4 Non-Compliance. It can be argued that most of the risk	Agreed

is from insiders, so doing personnel risk assessments is at least at vital as the other aspects mentioned in Level 4.

004-C2,4

CIP004 - Personnel and Training

Name Scott R Mix

Entity KEMA

Comments		***Responses***
General	The compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).	Done in Draft 3
004-R1	Requirement R1. Insert the word “quarterly” before the word “on-going”.	Accepted
	Requirement R1. Insert “including contactors and service vendors” after “personnel”	
	Requirement R1. Add the following phrase to the end of the requirement: “as the practices apply to the Critical Cyber Assets covered by this standard”	
004-R2	Requirement R2. Insert “including contactors and service vendors” after “personnel”	Accepted
004-R3	Requirement R3: replace “background screening” with “the results of the personnel risk assessment process”	Accepted
	Requirement R3. Insert “including contactors and service vendors” after “personnel”	
004-R4		
004-M1		
004-M2	Measure M2. Change to read: “Training -- the Responsible Entity shall develop and maintain a company-specific cyber security training program, and review it’s contents annually, that includes …”	Measures & Requirments were all modified in Draft 3
	Measure M2.1: Add the following phrase: “as developed for the Critical Cyber Assets covered by this standard”	
004-M3		
004-M4	Measure M4.1: There is no requirement in standard CIP-004-1 relating to maintenance of a list of personnel and their access rights. This should be a requirement in standard CIP-003-1.	Measures & Requirments were all modified in Draft 3
	Measure M4.4: Change the first sentence to read, “The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel covered by this standard prior to being authorized access …”	
	Measure M4.6 replace “conduct update screenings” with “re-evaluate personnel risk assessment results”	

CIP004 - Personnel and Training

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Terry Doern
Entity	Bonneville Power Administration, Department of Energy

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4	R4: Add 'If background checks cannot be completed prior to access, they shall be escorted at all times.'	Not appropriate in this standard – a physical access issue.
004-M1		
004-M2		
004-M3		
004-M4	M4.4 This measures requires a 7-year criminal check versus the normal 5-year criminal check. In accordance with BPA Human Resources Personnel Letter No. 731-1 dated July 2, 2004, the current National Agency Check and Inquiries (NACI) performed for all new BPA employees and the equivalent performed for contractors is only 5 years. BPA performs the minimum federal background investigation for suitability for federal employment. This is also true for the background investigations for 'Public Trust' positions. Recommendation: Change to 'five year criminal check' versus seven, or add a comment - 'may be less than 7 years because US, state or local regulations may take precedence .' M4.6: DOE cannot perform timely background checks for this quantity of employees, to meet this standard. BPA may need to write an exemption.	All Requirements moved from Measurements; all personnel risk assessments
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		

CIP004 - Personnel and Training

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name	Todd Thompson
Entity	Southwest Power Pool

Comments		***Responses***
General		
004-R1		
004-R2	M2.4 -- this is a new requirement and there is no matching requirement in this standard.	Modified in Draft 3
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003.	All are modified in Draft 3
	M4.6 -- this should refer to risk assessment as in R4 rather than screenings.	
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	2.3.1 -- Please include a matching requirement or delete this paragraph.	Modified in Draft 3
004-C2,4		

CIP004 - Personnel and Training

Name Tom Pruitt

Entity Duke Power Company

	Comments	*Responses*
General	Overall -- Effective date of 10/1/05 for this standard is probably reasonable. A - 4 -- typo? Any reference in this Standard to Critical…. Why is this repeated here and in A - 3 ?	
004-R1		
004-R2		
004-R3	R3 -- Clarify requirements for Responsible Entity to retain records for contract employees. These employee records are typical created and retained by the contracting agency, not the Responsible Entity.	Responsible Entity is responsible for ensuring contractors comply with requir
004-R4	R4 -- Clarify this requirement or a "risk assessment"	Clarified in Draft 3
004-M1		
004-M2		
004-M3		
004-M4	M4.4. This requirement is an impediment to the rapid response requiring the intervention of a vendor and should be dropped. Further, it is discriminatory since some employees would be checked more rigorously than others and the minimum requirements would produce no reasonable assurance that a person is not a security risk. M4.2 -- Seven days may be difficult in some cases to achieve. M4.3 -- Seven days may be difficult in some cases to achieve. M4.4 -- Do we have to conduct background screenings on current employees? M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).	Establishes a minimum baseline

CIP004 - Personnel and Training

M4.6 -- Uses term "screening". Term "risk assessment" is used elsewhere. Be consistent. Requiring updated screenings every five years is burdensome and will provide no reasonable assurance that a person is not a security risk. What would update screenings entail?

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP004 - Personnel and Training

Name Tony Eddleman

Entity Nebraska Public Power District

Comments		***Responses***
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	Under section M4.6 - Delete the requirement for update screenings every five years and require the update screenings for cause only.	No grandfathering accepted – see FAQ#1 to this Standard.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name Tony Kroskey

Entity Brazos Electric Power Cooperative

Comments		*Responses*
General		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	Measure M4.4 describes a background check and criminal check as required. If this is a requirement then it should be stated in R4 and M4.4 would say that documentation is on-hand showing that the checks were completed.	Personnel risk assessment moved to Requirments section in Draft 3
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

Name	Trevor Tidwell	
Entity	Texas-New Mexico Power Company	
Comments		***Responses***
General		
004-R1		
004-R2	The Training requirement, R2, states that all personnel having authorized access to Critical Cyber Assets shall be trained etc. Does authorized access include access to a web server using an Internet browser? Or does it only include access that allows to users to make changes to the system? The wording of authorized access to Critical Cyber Assets is broad and vague. Either it needs to be specified personnel having authorized access regardless of type (i.e. read-only, or view-only) to Critical Cyber Assets shall be trained etc. Or a caveat needs to be included for read-only access.	See definitions and FAQ's for clarification
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP004 - Personnel and Training

CIP004 - Personnel and Training

Name William J. Smith

Entity Allegheny Power

Comments		***Responses***
General	The purpose states that personnel having authorized access to Critical Cyber Assets are required to have a higher level of screening, etc… than personnel not provided access. This is too prescriptive given the entity's responsibility to develop its own training program.	Sets a baseline
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	M4.4 - Reference to company personnel is confusing and should be clarified. Appears to imply that only employees need to have a personnel risk assessment while the implication of the standard is that all personnel (employee, contractor, vendor) who have unescorted access to critical cyber assets must have a personnel risk assessment completed.	
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		

CIP004 - Personnel and Training

004-C2,4