CIP-003 Drafting Team Responses to Comments

Commentor Bob Wallace
Entity Ontario Power Generation

	Comments	***Responses***
General	OPG feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The purpose of a policy is to inform all personnel working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate	This section and its corresponding requirement has been re-written.

	relationships>> too frequently. We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed. We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.	Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Carol L. Krysevig
Entity Allegheny Energy Supply Company

	Comments	*Responses*
General	General Comment -- Confusion throughout this section in terms of understanding the difference between critical information about the Critical Cyber Asset (floor plans, etc.) vs. critical information emanating from the asset that is vulnerable to attack or acquisition by a hacker. Is the Standard asking us to categorize only the first type, or both? Allegheny Energy believes the Standard's intent is to protect the information ABOUT the Critical Cyber Asset. Can you please clarify?	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2	R2.1 - Most Power Plant documentation contains significant amounts of information, cyber and non-cyber that could be used to hinder plant operation. The responsibly entity should be allowed to apply the same security measures to cyber documentation that it applies to other types of plant equipment and operating documentation.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3	R3. (Second paragraph)-- Not sure how to define a Critical Cyber Asset custodian. Can clarification be made on the term custodian?	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R4	R4.1 -- This item actually addresses two different items: a) Replacement systems and b) patches/changes to existing systems. Allegheny Energy recommends that the responsible entity establish security guidelines for new or replacement systems in lieu of the exact requirements defined here. R4. 1 Testing and assessment of patches/changes should be allowed to be done by third parties on non-production systems.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		

CIP-003 Drafting Team Responses to Comments

CIP-003 Drafting Team Responses to Comments

Commentor Dennis Kalma
Entity Alberta Electric System Operator (AESO)

	Comments	***Responses***
General		
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	1. It is not clear how compliance would be measured for this requirement -- what is significant risk? 2. Does it matter who in the company authorizes revocations and changes? 3. Is this authority "delegatable" during absences of the authorized person? Is it local company policy that applies?	1. The Requirements, Measures and levels of non-compliance have been modified. 2/3. A designated senior manager or designated delegate.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

CIP-003 Drafting Team Responses to Comments

Commentor Don Miller / Ray Morella
Entity FirstEnergy Corp

	Comments	*Responses*
General	Some of the Measures do not match up with the requirements, the timing for reviews, data retention periods, and senior management designation, etc are spelled out in the measures and omitted in the requirements. The measures should match the requirements!	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		

CIP-003 Drafting Team Responses to Comments

CIP-003 Drafting Team Responses to Comments

Commentor Earl Cahoe
Entity Portland General Electric

	Comments	*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4	Requirements, R4 Comment: This will be extremely expensive to implement, especially if the support for the critical cyber asset is outsourced. Recommendation: in R4.2, remove the word "all" before the word "hardware" in the first sentence. This can be extremely expensive to implement for some devices.	This section has been reworded. Even if the support is outsourced, the outsourced organization should have these types of controls in place to ensure that their customer is not harmed by shoddy practices.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Edwin C. Goff III
Entity Progress Energy

	Comments	*Responses*
General		
003-R1		
003-R2	R2 & R3 -- These requirements to categorize information and classify/control relative to sensitivity appear to be new requirements over and above the urgent action 1200 standard. These requirements are projected to require significant effort to implement and maintain such a document control system. However, the implementation plan requires Balancing Authorities to be Audibly Compliant by 1st QTR 2006. We would request that compliance for these requirements be changed to Substantially Compliant R2.2 - Clarification requested - Should categorizing information be based on various categories of "unauthorized personnel" that information may be disclosed? Please expand upon "relative sensitivity of information" that should not be disclosed; is this that information should be labeled "Classified", "Secret", "Top Secret", etc? Can the Drafting Team recommend an example system or process to use as a guiding reference?	This requirement is now R4. R4.2 now states "The Responsible Entity shall classify information related to Critical Cyber Assets based on sensitivity." It is up to each entitiy to determine how to classify it's information based on the enitity's determination of the sensitivity of the information.
003-R3	R2 & R3 -- These requirements to categorize information and classify/control relative to sensitivity appear to be new requirements over and above the urgent action 1200 standard. These requirements are projected to require significant effort to implement and maintain such a document control system. However, the implementation plan requires Balancing Authorities to be Audibly Compliant by 1st QTR 2006. We would request that compliance for these requirements be changed to Substantially Compliant	The part of this requirement that requires the defining of roles and responsibilities of critical cyber asset owners, custodians, and users has been removed. The implementation plan has been revised to compensate for the additional requirements in these sets of standards.
003-R4	R4 - Clarification requested - Does "software patches/changes" also include database changes such as adding new records or defining new tables? This requirement to establish a governance process appears to be new requirements over and above the urgent action 1200 standard. These requirements are projected to require significant effort to establish a documented process. However, the implementation plan requires Balancing Authorities & Reliability Coordinators to be Audibly Compliant by 1st QTR 2006. We would request that compliance for these requirements be changed to Substantially Compliant	Software patches/changes refers to the upgrading/changing/patching of application or operating system software. This does not apply to data entry or modification to tables. However, this would apply if you were to change/patch the underlying database code. A governance process is defined in R1 as a structure of relationships and decision-making processes and referred to in Levels of Non-Compliance 2.4.4. A governance process would have also been part of Sarbanes-Oxley compliance.
003-R5	R5.1 - Clarification requested - Does this requirement include documenting access authorizations to substation IED's (if the IED is located in a Critical Asset such as blackstart substation) ? What level of documentation is required, is this a list of named individuals? Pursuant to CIP-004, R4 would these individuals be required to complete background checks or personnel risk assessments? R-5 B Do the change management and testing requirements apply to all application software changes no mater how small. For example if an alarm set point is changed, one field in one record,	If the substation IED is contained within a defined physical security perimeter protecting a Critical Asset, then documenting access authorizations to substation IED's would be required. Yes, this is a list of named individuals that have the authority to authorize access to your Critical Cyber Assets. Typically, this would be a manager responsible for that asset(s).

	does that have to be tested in a non production environment. How big would an application software chance need to be to trigger the testing requirements..	Any individual with access to Critical Cyber Assets would be required to undergo a personnel risk assessment to at least the minimum requirements of these standards.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Francis J. Flynn, Jr., PE
Entity National Grid USA

	Comments	*Responses*
General	National Grid feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question. In section D of compliance 2.1.4 references 'an information security protection prgram exists but has not been reviewed in the last calendear year'. National Grid cannot find a Requirement within the standard that this is required. The Drafting Team must clarify and clearly explain and document what the requirement is.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft. This section has been revised so that compliance measures match up to requirements.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.

CIP-003 Drafting Team Responses to Comments

003-M11		
003-M12		
003-M13	We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently. We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed. We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.	This section and its corresponding requirement has been re-written. Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	In section D of compliance 2.1.4 references 'an information security protection prgram exists but has not been reviewed in the last calendear year'. National Grid cannot find a Requirement within the standard that this is required. The Drafting Team must clarify and clearly explain and document what the requirement is.	
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Gary Campbell
Entity MAIN

	Comments	*Responses*
General	M3 - M18 These measures as stated are really requirements and should be put there. The measures should be looking for these review times, documents with cetain requirement specifications, etc. Levels of Compliance Specifiy review times in the requirements Reguirements should state the minimum items the entity is to address, the measures should look to measure the global items such as plans, procedures, actions, etc. And levels of compliance should asses these measures.	These concerns have been addressed in the version 3 draft/
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	In M1, as an auditor I would only be looking for a Cyber security policy which states the commitment to protect Critical Cyber Assests, nothing more.	As an auditor as well, I would compare the measure to the requirement to ensure that the requirements have been appropriately met. The requirements and measures in this standards have been re-written to be more specific
003-M2	M2 This should be made into a requirements with the measure looking for the review times. I also think it should not be so undefinable.	The standard has been re-written to address these inconsistencies
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		

CIP-003 Drafting Team Responses to Comments

003-M13

003-M14

003-M15

003-M16

003-M17

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Gerald Rheault
Entity Manitoba Hydro

	Comments	*Responses*
General	Standards CIP-003 & CIP-007 need to be better coordinated in order to avoid existing confusion, overlap and redundance between the two standards. Suggested improvements are: 1. Rename CIP-003 Security Management removing the word "controls" to imply that this standard contains the high-level policy and governance requirements. 2. Rename CIP-007 Systems Security Controls replacing the term "Management" with "Controls" to reduce conflict with CIP-003 and imply that standard CIP-007 has more technical requirements versus the management requirements in standard CIP-003. 3. CIP-003 R4.2, a repeat of CIP-007 R8.1, should be deleted and left in the more technical standard CIP-007. CIP-003 uses the term "Executive" while other cyber secuirty standards use the terms "senior management" or "senior management official". One term should be used for all the cyber securtiy standards. Adding the word Senior in Senior Management really has little value.	All of the standards have been reworked as a set in order to reduce redundancy and provide greater clarity to the requirements of these standards.
003-R1	CIP-003 R1 should not refer to "this standard" or governance "controls". Suggested wording change to:"The Responsible Entity shall create and maintain a cyber security policy which includes governance that addresses the requirements of the cyber security standards."	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R2	CIP-003 R2.1 from "The Responsible Entity shall identify and protect all information, regardless of media type, related to the entity's Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes procedures, Critical Asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information." Removing the last sentence " These documents must be protected as well." and changing the first sentence to include "…identify and protect…". In CIP-003 R2.2 and R.2.3 use both the terms "categorize" and "classification". We suggest using only the term "classification". Change CIP-003 R2.2 to shorten and clarify as follows: "The Responsible Entity shall classify criticial cyber asset information based on sensitivity; to facilitate that only authorized access occurs." Delete CIP-003 R2.3 "Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity." This requirement is redundant with R2.1 and R2.2.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R3	In CIP-003 R3 change "designate delegate" to "designated delegates" (pural).	The requirements section has been reworked for clarity and consistency with other sections and standards

CIP-003 Drafting Team Responses to Comments

003-R4	In CIP-003 R4.2 suggest replacing "minimal security configuration standards" to "responsible entity's security configuration standards". Testing should also ensure a working functional system before going into production not that just security is in place	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R5	In CIP-003 R5 Change to "The Responsible Entity shall institute and document a process for the	The requirements section has been reworked for clarity and consistency
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Gordon Pietsch
Entity Great River Energy

	Comments	*Responses*
General	CIP-003 contains language that is redundant/overlapping with CIP-007. These two should be combined into one.	These standards have been reworked for clarity and consistency
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Guy Zito
Entity NPCC CP9

	Comments	*Responses*
General	CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	NPCC Participating Members do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets,and it is recommended that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	NPCC Participating Members feel that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	NPCC Participating Members are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the	This section and its corresponding requirement has been re-written.

	structure of internal corporate relationships>> too frequently. NPCC Participating Members feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed. Also how does an organization document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.	Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Howard Rulf
Entity We Energies

	Comments	*Responses*
General	This standard overlaps 007. Examples are R4.1,4.2, M13.1, 13.2. Combine or eliminate the redundancies.	These standards have been reworked for clarity and consistency
003-R1		
003-R2	Remove section 2.3.4.	This section has been reworked
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor James W. Sample
Entity California ISO

	Comments	*Responses*
General		
003-R1	The last sentence in R1 should be deleted as it is redundant.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R2		
003-R3	The words “from the requirements of this standard" should be replaced by “from the requirements of the NERC CIP series of standards". The last sentence of paragraph two is redundant and should be deleted	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R4		
003-R5	“and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous. This instance of R5 is redundant and should be deleted as it is stated in R2.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove sections M5 & M6 because they are scope creep and are covered in M7	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M6		
003-M7	Suggest “procedures" in M7 and M8 be changed to “controls".	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M8		
003-M9		
003-M10	M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		

CIP-003 Drafting Team Responses to Comments

003-M13	M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14	M14 – This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M15	M15 – same comment as M10	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M16		
003-M17	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	1.3.4 – if this is required, it should be moved to a requirements section.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Jerry Freese
Entity American Electric Power

	Comments	*Responses*
General	All measures should have quarterly review process. In the compliance section, the data should be kept for two years instead of three years. Three years requires storing a huge amount of data for an extra year.	Measures changed to annual reviews. Data to be kept for the previous full calendar year.
003-R1		
003-R2	In R2.2, we believe the word "classify" should be used instead of "categorize." R2.2 could read: "The Responsible Entity shall classify information related to Critical Cyber Assets in order to determine the relative sensitivity of such information; as well as to aid personnel with authorized access in judging what information can be disclosed to others. "	Moved to R4 and change to read: "R4.2. The Responsible Entity shall classify information related to Critical Cyber Assets based on sensitivity."
003-R3	The second paragraph of R3 should be a separate requirement - not part of R3 or a sub-requirement to R3. This should then map to M12. In R3 "cyber security standard" is a proper noun, and should be capitalized.	Second paragraph has been deleted. "Cyber Security Standard" removed. Substituted "NERC CIP-003 through CIP-009 Standards."
003-R4		
003-R5	R5.2 belongs with the measures, instead of with the Requirements. Overall, it seems like M14 through M18 should be submeasures of a measure that lines up with R5.	All sections of this standard have been revised in order to ensure that requirements do not creap into measures.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.1 is more of a requirement than a measure. Should this be included in R4.1? Or a separate subrequirement for R4?	Agree. Reworded and moved to requirements.

CIP-003 Drafting Team Responses to Comments

003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	In Compliance 1.3.4, "Documented" should be "Document" and this should be two years instead of three years.	Changed to "1.3.1 The Responsible Entity shall keep data from the previous full calendar year."
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Jerry Heeren
Entity MEAG Power

	Comments	*Responses*
General	A3 - The term “bulk electric system" needs to be capitalized and defined in the Definitions Section of CIP-003-1. A definition of this term is suggested at the top of this document. I Other Comments --Requirements and Measures numbering scheme does not match.	The term bulk electric system is defined in the NERC Glossary of Terms Used in Reliability Standards Numbering scheme fixed
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14	M14 needs to be clarified. Perhaps its intent would be clearer if two simpler sentences were used in place of one very complicated sentence.	Deleted from measures. Re-worded into M5 of version 3 of this standard
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18		
003-C1,1		
003-C1,2		
003-C1,3	In the Compliance portion of this Standard, the Data Retention subparagraph 1.3.4 discusses documentation of mitigation strategies. However, the need for mitigation strategies is not established in any Requirement or Measure.	Deleted. Mitigation strategies part of R2.2
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Jerry Litteer
Entity INL

	Comments	*Responses*
General	The CIP standard treats the Process Control (SCADA) network as though it is an island in the middle of the Internet. In fact, the majority (99 %+) of SCADA networks are within the network boundaries of a corporate network. It should be made clear that the corporate network is the first line of defense for the SCADA network. This standard (nor any of the previous standards) incorporates the corporate network security into the overall security of the grid. You can not separate the two. The numerous yearly reviews that are required throughout the CIP standard should probably be consolidated into a new section of the standard. This would help focus the reviews and facilitate a single yearly security posture review. This would also help eliminate forgetting a review that is buried in another part of the standard. At least a summary review log should be included to make sure all is ready. Missing: There is no mention of comparing the list of authorized users against the production system or accounts. (CIP007 R3.4 semi-annually) Periodic review of accounts on the production system is essential. No mention of checking the integrity of the operating system (e.g. rootkit) (CIP007 R5 software integrity but no specifics). No mention of reviewing the audit logs for suspicious activity (CIP-005 M5.3 --document review was done but no frequency specified)	All sections have been reworked to provide greater clarity and consistency with the other standards in this series. We agree with your concerns and think that you will find draft 3 to be clearer and more concise with requirements and measures.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	R5.3 user access changes due to termination accomplished in a time frame not specified as compared to 24 hours as specified in 1300. CIP-004 M4.3 states 24 hours for termination change of access. These statements are inconsistent. A process should be in place that would monitor AND document what was done during any extended period.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1	M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets. This is a fairly weak requirement for a security policy. The policy needs to be viewed on its content not its mere existence. Since the "Guide Lines" are not finalized, the following should be noted. The policy(s) should address: how the corporation enforces the policy, scope of the implementation and coverage, what employee and vendor uses of the network and assets are allowed, what penalties can be imposed, methods of recourse or appeal. Above all, the policy must: make good business sense, be technically sound and enforceable, be available to employee /vendor and be technically sound and enforceable.	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization. While your suggestions are very good, it is not up to the drafting team to design corporate policies. Each entity will need to develop its own policies in support of these standards.

	The policy must also be signed by any one with access to the corporate assets (vendor, employee, backup site manager, etc.), whether these assets are part of a control system or not. With the growing focus on network/data security, it would make sense for the corporation to have a single Security Policy document. This document would be divided into special sections that discuss general IT, SCADA, HIPPA, etc. security policies. This keeps from having conflicting policies that confuse rather than help the overall security posture.	
003-M2	M2 Review of cyber security policy a minimum of 3 years changed from 1 year in 1300. Due to the number of procedural controls a more frequent policy review is suggested.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.1 and M13.2 current list of personnel authorized for production, and change control added -- better. There is no mention of comparing the list of authorized users against the production system or accounts. Periodic review of accounts on the production system is essential --CIP-007-1 R3.4 mentions semi-annually. It would be ideal if the Password files on the production and test systems were scanned each day to make sure verify the authorized accounts (user + application + system) were the only accounts on the systems.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14		
003-M15		
003-M16		
003-M17		
003-M18	M18 User access rights confirmed annually instead of ¼ year in 1300. This might be OK if checking against the production system more frequently but that is only ½ year (CIP-007-1 R3.4).	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		

CIP-003 Drafting Team Responses to Comments

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Jim Hansen
Entity Seattle City Light

	Comments	*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	M5-10: Is there a difference between the Cyber Security Program in M10 and the information security protection program in M5? We're getting confused between the Cyber Security Policy, the Cyber Security Program, information protection security program, Cyber Security Standard (mentioned in R2.3), etc. Ideally, we'd like the standard to contain easy to identify documents that we can uniquevicollay relate to between requirements, measures, and compliance. In general this standard is will written but we believe could be cleaned up in order to minimze confusion.	The entire measures section has been re-worked to remove those items identified as requirements and clean up the language in this section.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		

CIP-003 Drafting Team Responses to Comments

003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1: There is no way to avoid at least level 1 non compliance the way this is written. For instance, a Responsibility Entity with a senior management official designated 100% of the time meets the criteria of a senior management official was not designated for less than 30 calendar days. It should be recognized that staff may decide to leave and it may take several days to appoint someone as acting senior management, or appoint alternative senior management. We suggest that this be changed to 20 or more but less than 30.	Statement has been re-worded to state "A senior manager was not designated for ten or more calendar days, but less than thirty calendar days during a calendar year". The feeling here is that management will appoint an interim manager while a search for a permanent manager is conducted. 10 days should be ample time to appoint an interim manager.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Jim Hiebert
Entity California ISO

	Comments	***Responses***
General	M5-10: Is there a difference between the Cyber Security Program in M10 and the information security protection program in M5? We're getting confused between the Cyber Security Policy, the Cyber Security Program, information protection security program, Cyber Security Standard (mentioned in R2.3), etc. Ideally, we'd like the standard to contain easy to identify documents that we can uniquevicollay relate to between requirements, measures, and compliance. In general this standard is well written but we believe could be cleaned up in order to minimze confusion.	All sections have been reworked to provide greater clarity and consistency.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		

CIP-003 Drafting Team Responses to Comments

003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1: There is no way to avoid at least level 1 non compliance the way this is written. For instance, a Responsibility Entity with a senior management official designated 100% of the time meets the criteria of a senior management official was not designated for less than 30 calendar days. It should be recognized that staff may decide to leave and it may take several days to appoint someone as acting senior management, or appoint alternative senior management. We suggest that this be changed to 20 or more but less than 30.	This has been corrected. The minimum number of days has been changed to 10. Most companies will not allow their workforce to continue beyond this timeframe without a manager being in command for the interim.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Joe Weiss
Entity KEMA

	Comments	*Responses*
General	FAQ 1. This should explicitly state that the Cyber Security Policy should be specifically designed for Critical Cyber Assets (Control System Security Policy not a traditional IT Security Policy).	The drafting team has reworked the entire series of standards based on comments from other reviewers. With the convergance of IT business systems with SCADA systems, it is imperative that any cyber security policy be broad enough to include those areas where these systems converge.
003-R1	R1. The Responsible Entity shall create and maintain a Critical Asset cyber security policy… Having a security policy is insufficient to protect Critical Assets; it must be a security policy designed specifically for Critical Assets (control systems).	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R2	2.4.2 No Critical Assets cyber security policy exists Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3		
003-R4		
003-R5		
003-M1	M1. The Responsible Entity shall maintain its written Critical Asset cyber security policy stating its commitment to protect Critical Assets. Having a security policy is insufficient to protect Critical Assets; it must be a security policy designed specifically for Critical Assets (control systems). It is also inconsistent to not have a specific Critical Asset cyber security policy and yet maintain it has a commitment to protect those assets.	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2	M2. The Responsible Entity shall review the Critical Asset cyber security policy ….	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		

CIP-003 Drafting Team Responses to Comments

003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.2 A written Critical Assets cyber security policy has not been developed or reviewed in the last calendar year… 2.1.4 A Critical Assets information security protection program exists but has…	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor John Lim
Entity Con Edison

	Comments	*Responses*
General	The Measures are not properly aligned with the requirements. This makes the document hard to follow.	This disparity has been corrected.
	M-2 States a "no longer than 3-year period" for reviewing the cyber security policy. Non-Compliance Level 1 2.1.2 makes this an annual requirement. D 2.1.2 should be revised to reflect the 3 year review requirement.	While the measure calls for annual reviews, the level one non-compliance of no review for 3 years is due to the fact that most regions audit compliance on a 3-year cycle.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Karl Tammer
Entity ISO/RTO Council

Comments		*Responses*
General		
003-R1		
003-R2	The last sentence in 2.1 should be deleted as it is redundant.	This sentence has been deleted
003-R3	The words "from the requirements of this standard" should be replaced by "from the requirements of the NERC CIP series of standards".	This sentence has been reworded to "Exceptions to the cyber security policy"
	This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.	Sentence has been deleted.
003-R4		
003-R5	"and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous. This instance of R5 is redundant and should be deleted as it is stated in R2.	This sentence has been deleted
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove sections M5 & M6 because they are scope creep and are covered in M7	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M6	Remove sections M5 & M6 because they are scope creep and are covered in M7	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M7	Suggest "procedures" in M7 and M8 be changed to "controls".	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M8	Suggest "procedures" in M7 and M8 be changed to "controls".	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M9		

CIP-003 Drafting Team Responses to Comments

003-M11		
003-M12		
003-M13	M13.1 is a duplicate of M 12 M13.2 -- There is not a requirement for Change Management in this standard. This text should be moved to the requirements section.	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M14	M14 -- This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M15	M15 -- same comment as M10 (M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.)	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M16		
003-M17	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-M18	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004	Measures section has been completely reworked so that measures are ways to indicate compliance with the requirements. Requirements in the measures section have either been moved to the requirements section or removed completely.
003-C1,1		
003-C1,2		
003-C1,3	1.3.4 -- if this is required, it should be moved to a requirements section.	Compliance section has been completely reworked so that requirements in the compliance section have either been moved to the requirements section or removed completely.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Kathleen M. Goodman
Entity ISO New England Inc.

	Comments	*Responses*
General	ISO-NE feels CIP-003 needs a little more work before it is ready for ballot.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1	The last sentence in R1 should be deleted as it is redundant.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R2		
003-R3	R3 the words <<from the requirements of this standard>> should be replaced by <<from the requirements of the NERC CIP series of standards>>. The last sentence of paragraph two is redundant and should be deleted	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R4	R4.1-4.2 belongs in CIP007, and should be removed from CIP003.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R5		
003-M1	We do not agree with M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>> We do not agree with M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	.Remove sections M5 & M6 because they are scope creep and are covered in M7	The measures section has been reworked for clarity and consistency with other sections and standards
003-M6	.Remove sections M5 & M6 because they are scope creep and are covered in M7	The measures section has been reworked for clarity and consistency with other sections and standards
003-M7	Suggest <<procedures>> in M7 and M8 be changed to <<controls>>.	The measures section has been reworked for clarity and consistency with other sections and standards
003-M8	Suggest <<procedures>> in M7 and M8 be changed to <<controls>>.	The measures section has been reworked for clarity and consistency with other sections and standards
003-M9		

CIP-003 Drafting Team Responses to Comments

003-M10	M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	We are concerned that M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from M13.M13.1 is a duplicate of M 12 M13.2 --This belongs in CIP007 and should be removed.	This section and its corresponding requirement has been re-written. Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14	M14 -- This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	The measures section has been reworked for clarity and consistency with other sections and standards
003-M15	M15 -- same comment as M10	The measures section has been reworked for clarity and consistency with other sections and standards
003-M16		
003-M17	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004.	The measures section has been reworked for clarity and consistency with other sections and standards
003-M18	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004.	The measures section has been reworked for clarity and consistency with other sections and standards
003-C1,1		
003-C1,2		
003-C1,3	1.3.4 There is no stated requirement for this and should be removed.	The measures section has been reworked for clarity and consistency with other sections and standards
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Keith Fowler
Entity LG&E Energy Corp.

	Comments	*Responses*
General	We are in agreement with the comments submitted by the ECAR CIPP group.	Please see responses to comments from ECAR CIPP group.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor 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. Modify M7 to change “procedures" to “controls." Eliminate M5 and M6 as it overlaps with M7.	Measures section has been reworked
	Measures 15 and 10 are redundant, one of them must go. Eliminate Measures 17 and 18 as those acts are already addressed in Measures 4.1 and 4.2 of CIP-004.	
	Reflect corresponding requirement to complement Compliance 1.3.4	
003-R1	Delete last sentence in R1.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R2		
003-R3	In R3, the words “from the requirements of this standard" should be replaced by “from the requirements of the NERC CIP series of standards. Delete the sentence beginning with “Roles and responsibilities shall also…"	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R4		
003-R5	Delete R5 as it is redundant with R2.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1	Modify C.M1 to state: “The responsible entity shall maintain a written cyber security policy."	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7	Modify M7 to change “procedures" to “controls." Eliminate M5 and M6 as it overlaps with M7.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.

CIP-003 Drafting Team Responses to Comments

003-M8		
003-M9		
003-M10	NYISO feels that M10 is too prescriptive, and should be modified to require less information, i.e. name/title/date. Measures 15 and 10 are redundant, one of them must go.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	Remove M13.1 as it is covered in M12 (for 13.1) or overly prescriptive. Migrate M13.2 to requirements section. Remove statement from M13 “and that executive management is continually engaged in the process" as it cannot be measured.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14		
003-M15	Measures 15 and 10 are redundant, one of them must go.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M16		
003-M17	Eliminate Measures 17 and 18 as those acts are already addressed in Measures 4.1 and 4.2 of CIP-004.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M18	Eliminate Measures 17 and 18 as those acts are already addressed in Measures 4.1 and 4.2 of CIP-004.	
003-C1,1		
003-C1,2		
003-C1,3	Reflect corresponding requirement to complement Compliance 1.3.4	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Kenneth A. Goldsmith
Entity Alliant Energy

	Comments	*Responses*
General	Remove overlapping requirements, measurements and non-compliance from CIP-003. Levels of Non-Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7 and 2.4.8 are redundant with CIP007.	Agree. CIP007 reviewed for redundancy and changes made accordingly.
003-R1		
003-R2		
003-R3		
003-R4	Requirements R4.1 is redundant with CIP-007 R1, R2 R4.2 is redundant with CIP-007 R8, R8.1 and R8.2.	Agree. Sections re-worded in both standards to complement rather than conflict.
003-R5	R5.2 is redundant with CIP-007 R3.4.	Agree. Sections re-worded in both standards to complement rather than conflict.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	Measurements M13.1 - move to CIP007	Moved to requirements section R5 and re-worded.
	M13.2 is redundant with CIP-007 M7, M7.1, M7.2	Removed from Measures. Moved to R6
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3	2.3.3 clearly and distinctly defined - how do you measure	Removed
003-C2,4	2.4.5 - Executive management engagement cannot be measured, remove from document	Removed.

CIP-003 Drafting Team Responses to Comments

Commentor Kurt Muehlbauer
Entity Exelon Corporation

	Comments	*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4	The requirement for change management in R4.2 is nearly identical to CIP-007-1 R8.1. We recommend that change management only be defined as a requirement in one standard.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R5	R5 does not accurately describe the scope of R5.1 through R5.3. R5 describes management of access to information associated with Critical Cyber Assets. R5.1 through R5.3 describes management of physical and electronic access to Critical Cyber Assets. We recommend that the following be deleted from R5: …information associated with…	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor L.W. Brown
Entity Edison Electric Institute

	Comments	*Responses*
General	Definitions There appears to be a formatting problem – based on a comparison with the other Definition sections, the definition of Critical Cyber Assets should not be in bold.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4	R4. This entire Requirement is redundant here, as substantially identical material also appears in CIP-007.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R5	R5. This Requirement may be redundant here, as similar material appears at CIP-007-1 Requirement R3.4. However, in this case, it may be appropriate to address the issue here only.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	M5, M6, M8. The need for these three separate Measures is unclear – they all seem to be addressing the same issue using only slightly different wording: “review," “perform an assessment," and “assess … to ensure compliance." If there are differences, they need to be more clearly expressed, or the three Measures should be combined into one.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.1, M13.2. These two sub-requirements are redundant here, as substantially identical material also appears in CIP-007.	The compliance section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14		
003-M15		

CIP-003 Drafting Team Responses to Comments

003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	Compliance 1.3.2. In addition to the already mentioned diverse terminology regarding who is meant by the various terms describing a responsible person within the Responsible Entity, this factor implies that only one such person can be named for compliance purposes, despite the existence of multiple business entities or units under the corporate structure. Some of that division may even be required by FERC regulation. Where appropriate or convenient, Responsible Entities should be permitted to appoint multiple responsible persons.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted. A (meaning one) senior manager must be responsible for the program. The senior manager may delegate responsibilities. This person will be responsible to guide and implement the program. While we understand that there are FERC requirements regarding the separation of transmission personnel from power traders, etc. it is still within FERC requirements to have a single person designated as the manager responsible for ensuring that the requirements of these standards are satisfied.
003-C1,4		
003-C2,1	Compliance 2.1. Action cannot be taken instantaneously. Thus, there must be a reasonable lower bound to define noncompliance. It has been suggested that 21 days allows adequate time for personnel changes to be implemented and reflected. Compliance 2.1.4, 2.1.5. These appear to state the same point. They should be merged, or the intended difference must be clarified.	This has been corrected. The minimum number of days has been changed to 10. Most companies will not allow their workforce to continue beyond this timeframe without a manager being in command for the interim.
-003-C2,2	Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7, 2.4.8. These five sub-levels are redundant here, as substantially identical material also appears in CIP-007. However, 2.2.2 here uses the more appropriate calendar year, whereas CIP-007-1 Compliance 2.2.1.1 uses an unduly stringent semi-annual review period.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C2,3	Compliance 2.3.3, 2.4.5. The phrases “clearly and distinctly" and “engaged" are too subjective in the context used. At 2.3.3, it is not clear how an auditor is to determine whether a Responsible Entity’s judgment about clear and distinct definitions of roles and/or responsibilities is correct, or under what criteria. It would seem sufficient compliance if the employees, contractors, venders, etc. of the Responsible Entity actually do understand their roles and/or responsibilities. At 2.4.8, it is not clear how an auditor is to determine whether a Responsible Entity’s judgment about the “engagement" of executive management was appropriate, or under what criteria. If not done generally in each of the Definition sections, it would be more useful if these phrases were to be clarified by addition of language to the effect that interpretations of such qualitative terms will be acceptable for compliance purposes – even if they may differ from those of other Responsible Entities or of compliance auditors – as long as they are reasonable or justifiable under normal standards of business decision-making	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Larry Conrad
Entity ECAR Critical Infrastructure Protection Panel

	Comments	*Responses*
General		
003-R1		
003-R2	R2.1 Recommend removing the word "all" and recommend removing the last sentence, which is redundant in the existing language. Change to: The Responsible Entity shall identify information, regardless of media type, related to the entity's Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. The following documents must be protected: Procedures related to critical cyber assets, Critical Asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		

CIP-003 Drafting Team Responses to Comments

003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	Recommend deleting item D.2.1.1. Current language conflicts with Section C.M11, which allows 30 days to update the information. Therefore, failure to designate senior official for less than 30 calendar days is not a violation. Non-Compliance violation D.2.1.1 should be eliminated. C.M11 states: Changes to the current senior management official must be documented within 30 calendar days of the effective date.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Larry Conrad
Entity Cinergy

	Comments	*Responses*
General	CIP-003-1-- General Comment about this section. Many of the requirements are not available through existing legacy systems. Cinergy is working with a vendor on a new EMS system, which should be operational in mid to late 2007. Some clause should be inserted into the documentation to allow time for delivery of a new system on order, which can supply the required controls. For example, other sections state the requirement applies "if it is technically feasible." We suggest adding this type of language to requirements in this section.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2	R2.1.-- We recommend changing "Responsible Entity shall identify all information, regardless of media type..." to "Responsible Entity shall identify information, regardless of media type..." Eliminate the word "all". It is impossible to certify that ALL information is protected. This was also pointed out in Draft I. Requirement as written is impossible to comply with.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3		
003-R4	R.4.-- Documentation requirements here did not change from Draft I to Draft II. This will require approximately 1 FTE to manage all of the required documentation. These ongoing costs will not significantly increase real security. Recommend that the documentation requirements be reduced by eliminating some of the following: -- -- Formal process for promoting systems into production (covered in testing) -- -- Keeping separate governance process documentation for cyber security purposes (this is covered in other corporate documents). R.4.1.-- "...approving authority shall...verify...system meets...standards...prior to being promoted to...production environment." This requirement could easily cripple emergency restoration of EMS operation especially in after hour conditions, i.e., getting formal approval and documentation that a system has passed testing criteria in an after hours emergency.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		

CIP-003 Drafting Team Responses to Comments

003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3	Non-Compliance 2.3.4.-- It is Level 3 violation if the list of designated approving authorities is not maintained and up to date. This seems too harsh. Recommend that this be changed to a Level 3 violation if the list of designated authorities has not been reviewed or updated in the last 12 months.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Laurent Webber
Entity Western Area Power Administration

	Comments	*Responses*
General	Combine CIP-003 and CIP-007 into one requirement for security controls, testing, and validation.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2	R2.1: The sentence, (This includes procedures, Critical Asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information,) more correctly belongs as a definition of (Critical Information). R2.1: The last sentence, (These documents must be protected as well,) seems unnecessary.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3		
003-R4	R4.1: It is not clear what the term (assessment) refers to here. The balance of the requirement refers only to testing. Remove the word assessment from the first sentence because it is not clear to what degree or how individual utilities are to assess new or replacement systems and software patches/changes. If this is meant to give utilities leeway in determining which patches are appropriate for installation, state so clearly.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		

CIP-003 Drafting Team Responses to Comments

003-M16

003-M17

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Lawrence R Larson, PE
Entity Midwest Reliability Organization

	Comments	*Responses*
General	CIP-003 contains language that is redundant/overlapping with CIP-007. These two should be combined into one. Under Section 2 (Non-Compliance levels): eliminate 2.3.3 - it is too vague. Also, move the following down one level from their current position (make one level less severe): 2.3.2, 2.4.4, and 2.4.7.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Lee Matuszczak
Entity U S Bureau of Reclamation

	Comments	*Responses*
General	Consider combining CIP-003-1 with CIP-007-1. Both standards discuss security management and management controls. Numbering errors lend confusion to the requirements in this standard. Multiple occurances of R3, R4, and R5 are noted.	The entire series of standards have been reworded. In draft 1 and 2 the drafting team worked in sub groups in order to begin to craft these standards. In draft 3, the sub groups came back together and as an entire team we looked at each standard. We removed redundant information and clarified requirements. Numbering errors have been corrected.
003-R1	R1. - The use of the term "bulk electric system" may be more applicable to all situations if changed to "critical non-cyber assets". This term will need to be defined in terms of some criteria, however (e.g., CIP-002-1 R1.2 through R1.11.)	Term has been removed from this section
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		

CIP-003 Drafting Team Responses to Comments

003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	D. Compliance 1.3.4 - It is unclear what this item is requesting "Documented review results of this standard and mitigation strategies for the information security program." Certainly it is possible to maintain records and documents associated with reviews, but "review results of this standard?"	The compliance sections have been reworded. It merely states that the responsible entity shall keep data from the previous full calendar year. This means that wherever the standard calls for documentation, that documentation must be retained for a full calendar year.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Linda Campbell
Entity FRCC

	Comments	*Responses*
General	If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?	Exceptions refer to a Responsible Entity's cyber security policy, not the standard. Duly authorized exceptions, as explained in CIP-003, R3 will not result in non-compliance to the standard. Having senior management review and approve exceptions demonstrates that a system of governance exists and senior management is aware of the risks of not being in full compliance due to technical or practicality issues.
003-R1		
003-R2		
003-R3		
003-R4	R4.1. It is not reasonable to authorize and document test results for routine maintenance changes. For example, Windows updates follow a fixed and repeatable procedure. Standard update procedures should not require formal authorization and documentation steps. Alternate wording could be Responsible Entities shall identify the controls for testing and assessment of new or replacement systems. Responsible entities shall designate approving authorities that will formally authorize and document that a system has passed testing criteria. The approving authority shall be responsible for verifying that a system meets minimal security configuration standards prior to the system being promoted to operate in a production environment. Routine software patches/changes are controlled and document via procedures. Formal approval is done only for initial implementation of the procedure.	This requirement has been moved to R6 and re-worded to allow the responsible entities to determine their own change management processes for changes to existing systems. It is typically not prudent to implement a "Microsoft" fix without testing it first. Microsoft patches have been known to break applications as well as Windows itself. Keep in mind that this only applies to Critical Cyber Assets and no necessarily the entire corporate enterprise. The standard requires the designation of an approving authority. There could be a number of people responsible for testing patches before implementation. The idea here is that you document that fact that the patch was appropriately tested according to your testing methodology and that having passed testing criteria, is deemed qualified to be placed into a production environment. The formal authorization and documentation of the testing provides proof that reasonable steps were taken to protect the envrionment from errant software patches. Better to bring down a test environment than production. Please reference R6 of draft 3 for changed wording.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		

CIP-003 Drafting Team Responses to Comments

003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1	The words under D1.1.2. really belong under D1.1.3. Data Retention. D1.1.2. 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. D1.1.3. should be as follows: D1.1.3. Data Retention The compliance monitor shall keep audit records for three (3) calendar years. The Responsible Entity shall keep data for three (3) calendar years and make the following available for inspection by the compliance monitor by request:	Compliance section has been re-written. Responsible Entity shall keep data from the previous full calendar year. Compliance monitor shall keep audit records for three calendar years.
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Lyman Shaffer
Entity Pacific Gas and Electric Company

Comments		*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	M5 & M10 -- M5 uses the term "information security protection program" and M10 users the term "cyber security program", was this intended? If so, why? If not, this needs to be fixed	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	M5 & M10 -- M5 uses the term "information security protection program" and M10 users the term "cyber security program", was this intended? If so, why? If not, this needs to be fixed	The measures section has been re-written to address these issues.
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		

CIP-003 Drafting Team Responses to Comments

003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1 "for less" should be changed to "for more than"	this section has been fixed.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Marc Butts
Entity Southern Company, Transmission, Operations, Planning and EMS Divisions

	Comments	*Responses*
General	Definitions of Terms -- The term Access needs to be defined and used more precisely in the associated text of this standard. Access can mean admission to physical locations, contact with information, ability to view/modify software code and/or data, authorization to log-in and execute a program, etc. The applicable access meanings should be captured more explicitly in the Definitions, and appropriate adjectives reflecting that meaning used in the text of the requirements and measures. Definitions of Terms -- The term Logical to reflect Electronic Security in the Purpose of CIP-005-1 is used in this standards R5.1 but never defined in this standard. Requirement 2 of this standard calls for an information protection program as a control for sensitive information concerning critical cyber assets. However, several measures and non-compliance levels go off into very vague subtleties. For example, consider combining measures M5, M6, and M8 into one simple measure that calls for an annual assessment of the information protection control to insure its effectiveness. It is a source of confusion to have 3 measures around this, one calling for an annual review (M5), one calling for an annual assessment (M6), and one calling for an annual -make sure the procedures comply- (M8). Along these same lines, under Level 1 Non-Compliance consider combining 2.1.4 and 2.1.5.	The drafting team has attempted to define common terms by their usage in place. Any specific definitions defined in the definition of terms section will become part of the NERC glossary of terms. Logical access is understood by most experienced network and cyber security personnel to mean access to electronic assets and/or information. It is unneccessary to redefine a commonly understood term. Requirements, measures and compliance sections have been reworked to be synchronized more closely with one another. Any requirements have been moved or removed from the measures and compliance sections
003-R1		
003-R2	Pg 3 of 8, R2.1; Regarding - could impact the reliability - This is very broad and subject to interpretation.	This section has been reworded.
003-R3		
003-R4	Pg 4, Re R4.1.: How will companies comply with this, especially for vendor supplied patches or upgrades? There is no measure associated with this requirement that the approving authority verifies a system meets minimum security configuration standards. Was this omission intentional?	There has to be a method to ensure that any changes made to the production environment do not adversly impact operations. Even vendor supplied patches should be tested before implementing into production. That being said, this section has been reworded.
003-R5	In R5 -- What information about a Critical Cyber Asset is this requirement referring to? Is it the information related to R2.1?	This section has been clarified and reworded.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		

CIP-003 Drafting Team Responses to Comments

003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.2 -- Change -all the Responsible Entity follows- to -all the Responsible Entities follow-, or just drop the word all.	Measures section has been reworked to be less prescriptive and clarified. Identified requirements in this section has been moved or deleted.
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1 (Level 1 Non-Compliance)-- All measures must have a reasonable lower bound and not be left open-ended such as -less than 30 calendar days-. In the event of a sudden absence of the senior management official (death, severance, etc) the standard should allow for an appropriate amount of time to appoint a replacement and complete the documentation. Suggested measure for L1 non-compliance is going more than 14 days but less than 1 month in aggregate during the year without a SMO named.	This has been corrected. The drafting team felt that more than 10 days without someone being placed in control during the interim was more than adequate. No business will allow its employees to work without a chain of command and decision making processes.
-003-C2,2		
003-C2,3	In Levels of Compliance, Level 3, items 2.3.3 and 2.3.4, the Roles and Controls that are to be defined/identified for compliance were not enumerated in the data that was to be retained per the Data Retention section so how would testing of compliance occur if an entity failed to retain this needed data?	These sections have been reworded for clarity and consistency
003-C2,4	2.4.5 (Level 4 Non-Compliance)-- There is no way to objectively measure and audit against the statement - Executive management has not been engaged in the cyber security program. These levels must be defined in such a way that an outside audit team can come in and objectively assess through observance of documentation or other factual data an appropriate non-compliance level. Delete this from L4.	These sections have been reworded for clarity and consistency

CIP-003 Drafting Team Responses to Comments

Commentor Patrick Miller
Entity PacifiCorp

	Comments	*Responses*
General	For the section B, R2, the subsections are inconsistent with the outline numbering format as R1 through R3 where they should be R2.1 through R2.3 instead. This should be modified to adhere to the correct outline format. For the section B, R4, the subsections are inconsistent with the outline numbering format as R4 and R5 where they should be R4.1 and R4.2 instead. This should be modified to adhere to the correct outline format. For the section B, R5, the subsections are inconsistent with the outline numbering format. Items R6 through R8 should either be in line with the R5 with respect to the indentation, or represented as subsections R5.1 through R5.3 to correctly adhere to the outline format. For section C, M13, there are two subsections R1 and R2 listed. These subsections should either be in line with respect to the indentation and listed as M14 and M15 or they should be represented as subsections of M13. If these are not subsections of M14, then the rest of the measures should be adjusted respectively.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6	For section C, M6, it is stated that “The Responsible Entity shall perform an assessment…" -- there is no mention of the type or scope of assessment required. The standard “risk based assessment" language should be used.	This has been corrected. Each entity will use a risk based assessment methodology that it determines best identifies its critical assets. EEI has recently published a risk assessment methodology that may work for this industry.
003-M7		
003-M8		
003-M9		

CIP-003 Drafting Team Responses to Comments

003-M10		
003-M11	For the section C, M11, within an organization of our size it may be more appropriate to have a 60 or even 90 day window for update.	The drafting team has set the lower limit to 10 days. Most companies will designate an interim manager to guide the flow of work and provide leadership to the employees. It would be considered irresponsible for and entity to not have someone in a leadership position assume responsibility for the interim until a more permanent replacement could be found. This manager must be documented within 30 days of being placed in that position.
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Paul McClay
Entity Tampa Electric

Comments		*Responses*
General	M3, M4, D.1.3.3 - “Exemptions" is a term used in the Measures M3, M4 (used twice) and Compliance D.1.3.3. This term is used no where else and is not defined. It should say exceptions or deviations. Also Refer to FRCC Comments	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Pedro Modia
Entity Florida Power and Light

	Comments	*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4	R4.1. It is not reasonable to authorize and document test results for routine maintenance changes. For example, Windows updates follow a fixed and repeatable procedure. Standard update procedures should not require formal authorization and documentation steps. Alternate wording could be: Responsible Entities shall identify the controls for testing and assessment of new or replacement systems. Responsible entities shall designate approving authorities that will formally authorize and document that a system has passed testing criteria. The approving authority shall be responsible for verifying that a system meets minimal security configuration standards prior to the system being promoted to operate in a production environment. Routine software patches/changes are controlled and document via procedures. Formal approval is done only for initial implementation of the procedure.	Testing requirements have been removed from this standard and moved to CIP-007
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		

CIP-003 Drafting Team Responses to Comments

003-M14

003-M15

003-M16

003-M17

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Pete Henderson
Entity Independent Electricity System Operator

	Comments	*Responses*
General	Renumbering of these requirements is necessary. The words “from the requirements of this standard" should be replaced by “from the requirements of the NERC CIP series of standards". Substantially greater care needs to be taken to ensure that the conditions leading to the various levels of non-compliance are a mutually exclusive set. This is not the case at present. This is very confusing and leads to an inability to understand which level an entity that is not in full compliance should certify to.	Numbering has been corrected and all sections of this and the other requirements have been reworked to reduce redundancy and provide clarity and consistency across all of the standards.
003-R1		
003-R2	The last sentence in R2.1 should be deleted as it is redundant.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R3	This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R4	In R4.2, the phrase, “and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous and should be deleted.	The requirements section has been reworked for clarity and consistency with other sections and standards
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove sections M5 & M6 because they are scope creep and are covered in M7. Furthermore, it is unclear what is meant by, “information security protection program" as no requirement to establish such a program has been specified.	The measurements section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M6		
003-M7	Suggest “procedures" in M7 and M8 be changed to “controls".	
003-M8		
003-M9		
003-M10	M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.

CIP-003 Drafting Team Responses to Comments

003-M11		
003-M12		
003-M13	M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section.	
003-M14	M14 – Delete the phrase, “to reflect any change in status that affects the designated personnel’s ability to authorize access to those Critical Cyber Assets" as it is redundant and confusing.	The measurements section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M15	M15 – same comment as M10	The measurements section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M16	See general comment on establishing review frequency based on risk considerations rather than prescribing an arbitrary frequency.	The measurements section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M17	M17 and M18 should be deleted. They duplicate measures 4.1 and 4.2 of CIP 004.	The measurements section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	1.3.4 – The need to establish a strategy has not been established as a requirement. If this is required, it should be moved to a requirements section and the term defined.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3	Failure to have a formal process to validate and promote systems to production (level 2 non-compliance) is equivalent to having no controls for testing and assessment of new or replacement systems (level 3 non-compliance).	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C2,4	2.4.7 is redundant and confusing. Failure to review access authorizations within a year is stated in 2.2.2 as leading to Level 2 non-compliance.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.

CIP-003 Drafting Team Responses to Comments

Commentor Randy Schimka
Entity San Diego Gas and Electric Co

	Comments	***Responses***
General	We think it would be helpful for the Requirements and Measures sections to have a one-for-one correlation to make the compliance process easier to organize and manage. M5 reference - Information Security Protection Program, M10 reference - Cyber Security Program, etc. Different terminology is used through the document to refer to the same Security programs as noted above. Please update naming conventions to make more consistent and easier to follow.	All sections have been reworked to provide greater clarity and consistency.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		

CIP-003 Drafting Team Responses to Comments

003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	Compliance section 2.1.1 - Senior management officials may change during the year, but this section seems to indicate non-compliance if a senior management official position is not occupied or designated for even 1 day during a transition. This wording seems to be in conflict with section M11.	This has been corrected. The minimum number of days has been changed to 10. Most companies will not allow their workforce to continue beyond this timeframe without a manager being in command for the interim.
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corporation (CHGE)

	Comments	***Responses***
General	CHGE feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8	CIP004 Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.	This entry belongs in the response to CIP-004v
003-M9		
003-M10	We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.	This section and its corresponding requirement has been re-written. Part of the new wording is "...that management is continually engaged in

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

003-M14

003-M15

003-M16

003-M17

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?

CIP-003 Drafting Team Responses to Comments

Commentor Richard Engelbrecht
Entity Rochester Gas and Electric

	Comments	*Responses*
General	CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	NPCC Participating Members do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets,and it is recommended that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	NPCC Participating Members feel that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	NPCC Participating Members are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the	This section and its corresponding requirement has been re-written.

	structure of internal corporate relationships>> too frequently. NPCC Participating Members feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed. Also how does an organization document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.	Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Richard Kafka
Entity Pepco Holdings, Inc. - Affiliates

	Comments	*Responses*
General	CIP-003-1: When compared to the other definition sections in the other standards there appears to be a minor formatting problem. The definition of Critical Cyber Assets should not be in bold. CIP-003-1 The phrases “clearly and distinctly" and “engaged" in Compliance 2.3.3 and 2.4.8 are too vague. How will an auditor judge whether any choice or level of “engagement" was appropriate? Further clarification/definition is needed. M5, M6, M8. Is there a need for these three separate Measures or can they be combined? The same issue appears to be addressed using only slightly different wording: “review," “perform an assessment," and “assess ...to ensure compliance." If there are differences, they need to be more clearly expressed.	Formatting has been corrected.
003-R1		
003-R2		
003-R3		
003-R4	R4. This entire Requirement is redundant here, as substantially identical material also appears in CIP-007.	Agree. Sections re-worded in both standards to complement rather than conflict.
003-R5	R5. This Requirement may be redundant here, as similar material appears at CIP-007-1 Requirement R3.4. However, in this case, it may be appropriate to address the issue here only.	Agree. Sections re-worded in both standards to complement rather than conflict.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.1, M13.2. These two sub-requirements are redundant here, as substantially identical material also appears in CIP-007.	M1.3.1 Moved to requirements section R5 and re-worded.

	M1.3.2 Removed from Measures. Moved to R6
003-M14	
003-M15	
003-M16	
003-M17	
003-M18	
003-C1,1	
003-C1,2	
003-C1,3	Compliance 1.3.2. Please reference the comment under definitions regarding the diverse terminology utilized to describe a responsible person (e.g. current designated senior management official) within the Responsible Entity. Does one individual have to be designated or can this be a shared designation/responsibility? Most large utilities have major operating subdivisions or lines of business (e.g. regulated T&D, unregulated Generation, and Corporate IT); some of that division may even be required by FERC regulation. Where appropriate or convenient, Responsible Entities should be permitted to appoint multiple responsible persons.
003-C1,4	
003-C2,1	Compliance 2.1. (Level 1): Action cannot be taken instantaneously, therefore there must be a reasonable lower bound to define noncompliance. Would suggest 21 days as a lower bound to allow adequate time for personnel changes to be implemented and reflected. Compliance 2.1.4, 2.1.5. These appear to state the same point. They should be merged, or the intended difference clarified.
-003-C2,2	Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7, 2.4.8. These five sub-levels are redundant here, as substantially identical material also appears in CIP-007. However, 2.2.2 here uses the more appropriate calendar year, whereas CIP-007-1 Compliance 2.2.1.1 uses an unduly stringent semi-annual review period.
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Commentor Robert Strauss
Entity New York State Electric & Gas Corporation

	Comments	*Responses*
General	NYSEG concurs with NPCC that CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8	CIP004 Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.	This entry belongs in the response to CIP-004
003-M9		
003-M10	We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate	This section and its corresponding requirement has been re-written.

	relationships>> too frequently. We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed. We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.	Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Roger Champagne
Entity Hydro-Québec TransÉnergie

	Comments	*Responses*
General	HQTÉ feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.	Standards have been reviewed by NERC technical writers and many suggestions have been made and adopted. The drafting team has made significant efforts based on the comments received to "clean up" version 3 of this draft.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1	HQTÉ does not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3		
003-M4		
003-M5	Please explain what <<information security protection programs>> C.M5 refers to.	This is clarified in R4 and M4 of version 3 of this draft.
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	HQTÉ feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	HQTÉ is concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate	This section and its corresponding requirement has been re-written.

	relationships>> too frequently.	Part of the new wording is "...that management is continually engaged in the process" (R1.3). This is easy to measure in an audit by asking a few simple questions such as do you have access to the company's policy or what is your process to keep management informed ?
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Roman Carter
Entity Southern Company Generation

	Comments	*Responses*
General	Definitions of Terms -- The term Access needs to be defined and used more precisely in the associated text of this standard. Access can mean admission to physical locations, contact with information, ability to view/modify software code and/or data, authorization to log-in and execute a program, etc. The applicable access meanings should be captured more explicitly in the Definitions, and appropriate adjectives reflecting that meaning used in the text of the requirements and measures. Definitions of Terms -- The term Logical to reflect Electronic Security in the Purpose of CIP-005-1 is used in this standards R5.1 but never defined in this standard. Requirement 2 of this standard calls for an information protection program as a control for sensitive information concerning critical cyber assets. However, several measures and non-compliance levels go off into very vague subtleties. For example, consider combining measures M5, M6, and M8 into one simple measure that calls for an annual assessment of the information protection control to insure its effectiveness. It is a source of confusion to have 3 measures around this, one calling for an annual review (M5), one calling for an annual assessment (M6), and one calling for an annual -make sure the procedures comply- (M8). Along these same lines, under Level 1 Non-Compliance consider combining 2.1.4 and 2.1.5.	The drafting team has attempted to define common terms by their usage in place. Any specific definitions defined in the definition of terms section will become part of the NERC glossary of terms. Logical access is understood by most experienced network and cyber security personnel to mean access to electronic assets and/or information. It is unneccessary to redefine a commonly understood term. Requirements, measures and compliance sections have been reworked to be synchronized more closely with one another. Any requirements have been moved or removed from the measures and compliance sections
003-R1		
003-R2	Pg 3 of 8, R2.1; Regarding - could impact the reliability - This is very broad and subject to interpretation.	This section has been reworded.
003-R3		
003-R4	Pg 4, Re R4.1.: How will companies comply with this, especially for vendor supplied patches or upgrades? There is no measure associated with this requirement that the approving authority verifies a system meets minimum security configuration standards. Was this omission intentional?	There has to be a method to ensure that any changes made to the production environment do not adversly impact operations. Even vendor supplied patches should be tested before implementing into production. That being said, this section has been reworded.
003-R5	In R5 -- What information about a Critical Cyber Asset is this requirement referring to? Is it the information related to R2.1?	This section has been clarified and reworded.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		

CIP-003 Drafting Team Responses to Comments

003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	M13.2 -- Change -all the Responsible Entity follows- to -all the Responsible Entities follow-, or just drop the word all.	Measures section has been reworked to be less prescriptive and clarified. Identified requirements in this section has been moved or deleted.
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1 (Level 1 Non-Compliance)-- All measures must have a reasonable lower bound and not be left open-ended such as -less than 30 calendar days-. In the event of a sudden absence of the senior management official (death, severance, etc) the standard should allow for an appropriate amount of time to appoint a replacement and complete the documentation. Suggested measure for L1 non-compliance is going more than 14 days but less than 1 month in aggregate during the year without a SMO named.	This has been corrected. The drafting team felt that more than 10 days without someone being placed in control during the interim was more than adequate. No business will allow its employees to work without a chain of command and decision making processes.
-003-C2,2		
003-C2,3	In Levels of Compliance, Level 3, items 2.3.3 and 2.3.4, the Roles and Controls that are to be defined/identified for compliance were not enumerated in the data that was to be retained per the Data Retention section so how would testing of compliance occur if an entity failed to retain this needed data?	These sections have been reworded for clarity and consistency
003-C2,4	2.4.5 (Level 4 Non-Compliance)-- There is no way to objectively measure and audit against the statement - Executive management has not been engaged in the cyber security program. These levels must be defined in such a way that an outside audit team can come in and objectively assess through observance of documentation or other factual data an appropriate non-compliance level. Delete this from L4.	These sections have been reworded for clarity and consistency

CIP-003 Drafting Team Responses to Comments

Commentor Scott R Mix
Entity KEMA

	Comments	*Responses*
General	There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Ensure that there are no requirements in Measures and no measures in Requirements. Required timeframes for review should be specified in Requirements (not Measures). Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual). FAQ CIP-003-1.Q1 should indicate that the special needs and considerations of Cyber Security Policy for Critical Cyber Assets covered by these standards needs to be called out and specifically addressed if it is to be included in a larger corporate policy set. In FAQ CIP-003-1.Q3, the lowest level of US Government classification is “Confidential", not “Classified". FQA CIP-003-1.Qnew: Does the list of personnel authorized to access or approve access to Critical Cyber Assets include vendors, contractors and consultants? In response to a question in Draft 1, it was indicated that reference to the ISA SP99 standard would be included in the FAQ portion of the standard. Please include this reference.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series. FAQs have been reworked as well.
003-R1	Requirement R1. Add the following sentence: “This cyber security policy should address the special requirements and needs of cyber assets as defined in Standard CIP-002-1." Requirement R1. Add the following: “This policy shall be approved and reviewed as often as determined by the responsible entity, with a period not to exceed 3 years. Any deviations or exemptions from this policy must be reviewed and approved annually by senior management to ensure the exemptions or deviations are still required and valid."	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R2	Requirement R2: Add the following: “, and review the program and assess it’s effectiveness annually."	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3		
003-R4		
003-R5	Requirement R5.1 should be split into two requirements. The first requirement should specify who is responsible to authorize individuals to access Critical Cyber Assets. The second requirement should be to maintain documentation of who is authorized to have access to the Critical Cyber Assets.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1		

CIP-003 Drafting Team Responses to Comments

003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15	Measure M15: add “affiliation (for vendors and contractors)" after “title"	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Steven L Townsend
Entity Consumers Energy

Comments		*Responses*
General	Please clarify sections R2.2 and R2.3, they are somewhat confusing.	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor Terry Doern
Entity Bonneville Power Administration, Department of Energy

	Comments	*Responses*
General		
003-R1	Requirement R1 is not titled.Recommendation: Title it 'Cyber Security Policy:'	Drafting Team has titled the requirements in this standard.
003-R2	Requirement R2 is not titled.Recommendation: Title it 'Information Protection Program:'	Drafting Team has titled the requirements in this standard.
003-R3	Requirement R3 is not titled.Recommendation: Title it 'Roles and Responsibilities:'	Drafting Team has titled the requirements in this standard.
003-R4	R4.1 Significant Issue: Requirement defines the role of the designated approving authority to formally authorize and document that the system has passed testing criteria and to for verifying that a system meets minimal security configuration standards. Under the NIST SP 800-37 'Guide for the Security Certification and Accreditation of Federal Information Systems', the designated approving authority (authorizing official) is the official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. Recommendation: Change this section to read 'Responsible entities shall designate approving authorities that will formally assume responsibility for operating the Critical Cyber Assets. The approving authority shall ensure a comprehensive assessment of the system's compliance with this standard has been performed to determine the extent to which the cyber security controls are implemented correctly and operating as intended. R4.1 Clarification Issue: The requirement mentions minimal security configuration standards but these are not clearly mentioned under CIP-005 'Electronic Security' or CIP-007 'Systems Security Management'. Recommendation: Update CIP-003, 005, and/or 007 to more clearly show the association between the responsibility to verify minimal security configuration standards and CIP-005 and CIP-007. R4.2 & M13.2 (repeated in CIP-007) Issue: Requirement CIP-007 R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed. Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)	This section is now part of requirement 6. Requirement 6.3 now reads "The Responsible Entity shall implement an approval authority responsible for formal sign-off on testing results prior to a system (new or modified) being promoted to operate in a production environment."
003-R5	Requirement R5 is not titled.Recommendation: Title it 'Access Authorization:'	Drafting Team has titled the requirements in this standard.
003-M1		
003-M2		

CIP-003 Drafting Team Responses to Comments

003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13	R4.2 & M13.2 (repeated in CIP-007) Issue: Requirement CIP-007 R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed. Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)	R4 has been moved to R6. This requirement has been modified to read "The Responsible Entity shall document the conrols for testing and assessment of new or replacement systems and software patches/changes." Measure M6 has been modified to coincide with the changes to R6.
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4	2.4.6 Issue: This is the first mention of the phrase 'corporate governance program'. Requirement R4 uses the phrase governance process. Recommendation: Include this phrase in Requirement R4 and Measure M13 for clarity.	Changed wording to 'No governance process exists'

CIP-003 Drafting Team Responses to Comments

Commentor Tim Hattaway
Entity AECoop

	Comments	*Responses*
General		
003-R1		
003-R2		
003-R3		
003-R4	In many cases, these systems will be purchased/installed from vendors. This requirement needs to make provisions for those systems. Responsible Entities should ensure all purchased software systems are adequately tested to secure its Critical Cyber Assets.	The requirements section has been re-worked for entities to institute a process of change control that should cover systems that are installed and/or purchased from vendors.
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		
003-M18		

CIP-003 Drafting Team Responses to Comments

CIP-003 Drafting Team Responses to Comments

Commentor Todd Thompson
Entity Southwest Power Pool

Comments		***Responses***
General		
003-R1		
003-R2	The last sentence should be deleted as it is redundant.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3	The words “from the requirements of this standard" should be replaced by “from the requirements of the NERC CIP series of standards" This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R4		
003-R5	“and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous. This instance of R5 is redundant and should be deleted as it is stated in R2.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove sections M5 & M6 because they are scope creep and are covered in M7	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M6		
003-M7	Suggest “procedures" in M7 and M8 be changed to “controls".	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M8		
003-M9		
003-M10	M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		

CIP-003 Drafting Team Responses to Comments

003-M12		
003-M13	M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14	M14 – This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M15	M15 – same comment as M10	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M16		
003-M17	M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-M18		
003-C1,1		
003-C1,2		
003-C1,3	1.3.4 – if this is required, it should be moved to a requirements section.	The compliance section has been reworked for clarity and consistency with other sections and standards. Compliance items that were identified as requirements have been either moved or deleted.
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Tom Pruitt
Entity Duke Power Company

	Comments	***Responses***
General	M4, M5, M6, M13: is annually really necessary? Will things change that often? It would be better to review AFTER significant changes or at a period not to exceed 3 years.	Measurments section has been completely reworked for clarity and consistency
003-R1		
003-R2	R2: looks like formatting (step numbering for sub-steps) is messed up. The first item under R2 probably should be R2.1, then R2.2, etc. Overall – Effective date of 10/1/05 for this standard is unrealistic due to requirement B R2.1 Creates administrative nightmare spanning multiple organizational departments/functional model entities.	The requirements section has been reworked for clarity and consistency with other sections and standards.
003-R3	R3 – What level is considered senior management? Is this one person for the entire company or can there be several?	The requirements section has been reworked for clarity and consistency with other sections and standards. A senior manager is a person that has the appropriate levels of responsibility and authority to guide the program. This is one person. However, that person can delegate responsibility. The senior manager identified will be ultimately responsible for the program. This is no different from the executives that sign off on your finacial statements being responsible for their accuracy (Sarbanes-Oxley controls)
003-R4	R4 – Says executive level management… all standards need to be consistent with management level requirements?	Wording struck.
003-R5		
003-M1	M1.4 – what is this trying to say?	This measure has been re-worded. The drafting team would suggest, however, that each entity include language in a policy that indicates management's support and commitment to protect critical cyber assets. The pupose of a policy is to inform all personell working for the responsible entity what is expected of them from a management perspective. These are defining principles of the organization.
003-M2		
003-M3	M3 – Senior management official ? Consistency…	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M4		

CIP-003 Drafting Team Responses to Comments

003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10	M10. Identity of the individuals should be just sufficient to uniquely identify the person. Titles and business addresses are subject to change and these events should not require an update of the program documents	Moved to requirements. This is essentially the same as it was in the 1200 Urgent Action. The standard calls for a senior manager to be in charge of the implementation and adherence to these standards. Requiring documentation as to the person's name, title, etc. enforces accountability for the implementation and adherence to the standards.
003-M11		
003-M12		
003-M13	M13 – Says executive level management… all standards need to be consistent with management level requirements? M13.2 – typo? …shall verify that all the Responsible … ?	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted.
003-M14		
003-M15	M15. Identity of the individuals should be just sufficient to uniquely identify the person. Titles and business addresses are subject to change and these events should not require an update of the program documents.	The measures section has been reworked for clarity and consistency with other sections and standards. Measures that were identified as requirements have been either moved or deleted. If titles and business addresses change, then you will need to update your documentation. These things should not be changing that often to cause problems.
003-M16		
003-M17		
003-M18		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
-003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Commentor Tony Eddleman
Entity Nebraska Public Power District

Comments		*Responses*
General	Under section R2.1 - A few SCADA vendors exist that provide systems across the globe. SCADA systems are used around the world and the majority of the documentation that will be classified by this document is readily available to "the bad guy".	As far as the SCADA vendor go , that may be true. However, your particular network topology, the layout of your computing center or operations center, disaster recovery plans, etc. will be unique to your environment. How you protect the information therein and how you protect access to your SCADA system needs to be protected. While the 'bad guy" may be able to obtain an understanding as to how your brand of SCADA functions, the actual compromise of your system should be a more difficult process if you have undergone the effort to secure the logical and physical access to your systems. Just because I can gain access to information on the physical workings of the locks on your house shouldn't guarantee that I would be able to gain entry. You might have an alarm system, a dog, or other means of protection that enhance the security of the locks. That would be information that should not be readily obtainable. To that end, this is what we are requiring you to protect.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		

CIP-003 Drafting Team Responses to Comments

003-M12

003-M13

003-M14

003-M15

003-M16

003-M17

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Commentor William J. Smith
Entity Allegheny Power

Comments		*Responses*
General	General Comment -- Confusion throughout this section in terms of understanding the difference between critical information about the Critical Cyber Asset (floor plans, etc.) vs. critical information emanating from the asset that is vulnerable to attack or acquisition by a hacker. Is the Standard asking us to categorize only the first type, or both? Allegheny Power believes the Standard's intent is to protect the information ABOUT the Critical Cyber Asset. Can you please clarify?	All sections have been reworked to provide greater clarity and consistency with the other standards in this series.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-M7		
003-M8		
003-M9		
003-M10		
003-M11		
003-M12		
003-M13		
003-M14		
003-M15		
003-M16		
003-M17		

CIP-003 Drafting Team Responses to Comments

003-M18

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

-003-C2,2

003-C2,3

003-C2,4