CIP-002 Drafting Team Responses to Comments

Commentor	Bob Wallace
Entity Name	Ontario Power Generation

	Comments	***Responses***
General	OPG strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. We suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system. >>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed.
002-R2		
002-R3		
002-R4	We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>	This requirement has been modified. The correspondending measure has also been modified.

CIP-002 Drafting Team Responses to Comments

	Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Option for a delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Option for a delegate(s) has been added.
002-C1,1		
002-C1,2	Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?	Compliance 1.2 has been modified to "Annually". Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Carol L. Krysevig
Entity Name	Allegheny Energy Supply Company

	Comments	***Responses***
General		
002-R1	R1. and R1.1. -- These items do not address the potential conflict if there are overlapping responsibilities between Responsible Entities. For example, can a Reliability Coordinator choose which assets belonging to or operated by a Generation Owner or Generation Operator are deemed Critical Assets? R1.6 and R1.7 -- Provide clarification regarding the difference between these two listed items (common control system vs. control center).	Each Responsible Entity must identify the Critical assets under its control.
002-R2	R2.1. - For the technically minded, this definition is pretty vague. For example, a PC running Windows NT that is not connected to anything else, may internally use TCP/IP for communications between separate programs running on that PC. By the current definition, this PC would be considered a Critical Cyber Asset. The definition should be more specific. For example, the following revision would clarify the Standard's intent: The Cyber Asset uses a routable protocol and is connected to a data network that is routing that protocol to a network connected outside the Electronic or Physical Security Perimeter. Another example is that DNP is a protocol that can be routed through the public telephone lines and tunneled through TCP/IP based networks. Allegheny Energy believes that an RTU having only a DNP via serial connection is not intended to be included on this Standard's critical cyber asset list.	R2.1 has been modified. Routable protocols has been clarified in the FAQs.
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Dave McCoy
Entity Name	Great Plains Energy Cyber Security Task Force

	Comments	***Responses***
General		
002-R1	Listing specific items as being included in the list of Critical Assets is not recommended, but if you are going to keep this list, we offer the following comments: R1.1.3 - the language is OK, but it would help to include or reference where to find the definition of "elements monitored as IROL's." R1.1.4 and R1.1.5 are unnecessary. Instead this should merely state any generator whose loss would cause instability, uncontrolled separation(s) or cascading outages. R!.1.7 - Why reference 300MW for load shedding? Wouldn't this be different for different size utilites? R1.1.9 - We are still waiting to see what is meant by "risk-based assessments." We've been promised some guidelines on this, but they have still not been produced.	IROL is defined in the NERC Glossary of Terms. The criteria that you use to define which generators must be covered requires significant events to have occurred. We want to have generators covered by the cyber security standards wefore such events may occur.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Dennis Kalma
Entity Name	Alberta Electric System Operator (AESO)

	Comments	*Responses*
General		
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6	If there are no critical cyber assets, the entity must still name a senior officer and do an annual review. i.e.: must have a program in place regardless of owning critical cyber assets.	R3 clarifies the requirements for a Responsible Entity with no Critical Assets or no Critical Cyber Assets.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Don Miller / Ray Morella
Entity Name	FirstEnergy Corp

	Comments	***Responses***
General	An additional document or section is needed showing "appropriate risk-based assessment methodology" for the entity's circumstances. This assessment methodology would further give the guidance and clearity to the environments included in the permanent standard. Also provide some consistenancy across the industry on what the critical items are and how NERC views their impact on the entity's environment and the country. This would not be an exact science since all the environments differ, only a guideline.	Suggesting an appropriate risk-based assessment methodology is outside the scope of the NERC Cyber Security Standards. The Standard does define a minimum set of critical cyber assests to act as a baseline.
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Earl Cahoe
Entity Name	Portland General Electric

	Comments	***Responses***
General		
002-R1	Requirements, R1.1.5 Recommendation: Need a definitive list of Regional Reliability Organizations. Define "largest single contingency" or give an example.	The largest single contingency is available from the Regional Reliability Organization.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2	Measures, M2 Recommendation: Please provide an example. Would a statement like "ABC Company used a qualitative risk assessment with xxx as the criteria" be sufficient?	Examples can not be included in a standard.
002-M3		
002-M4		
002-M5		
002-M6	Measures, M6 Recommendation: Add the words "or designee's" after "... senior management officer's ...". Adding a network device shouldn't require a senior VP's approval.	Option for delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Edwin C. Goff III
Entity Name	Progress Energy

	Comments	***Responses***
General		
002-R1	R1.1.4 - If multiple generating plants are located on the same site and share a common control room, do those individual plants have to be summed when determining if they meet the 80% Regional Reliability Organization contingency? These plants may or may not be generating at the same time. R1.1.7 - -- Clarification requested. - In the response to comments of the 1st draft of 1300, the Drafting Team indicated that NERC span of control does not include Distribution Systems. Please clarify that Distribution Systems capable of shedding in excess of 300MW of residential load control are excluded.	Generating plants must share a common system not just a control room. Each generating plant meeting the criteria must be protected whether generating at the same time or not.
002-R2	R2 - It is my understanding that requirement R.2.1. is intended to cover the situation where a networking capability (i.e. routable protocols) may be used to remotely access and/or control a Critical Cyber Asset in an inappropriate or unauthorized manner. A better way of defining the capability that may allow this to occur would be something like the following: "R.2.1. The Cyber Asset that can be accessed by unauthorized personnel, either inside or outside the controlled environment, that then may be manipulated, controlled, or otherwise utilized to remotely access and/or control any Critical Cyber Asset in an inappropriate or unauthorized manner." This definition would then cover the use of a routable protocol or any other means that may be used - with or without a routable protocol -- to inappropriately access and/or control a Critical Cyber Asset. For example, this would cover the use of a wireless connection mechanism that could be used to provide inappropriate access to a Critical Cyber Asset by unauthorized personnel outside the protected perimeter of the Critical Cyber Asset. In this case there would be no need for a routable protocol to allow the inappropriate and/or unauthorized access.	R2.1 has been modified.
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		

CIP-002 Drafting Team Responses to Comments

002-C1,3

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

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

	Comments	***Responses***
General	NPCC strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. We suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.>>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed.
002-R2	National Grid recommends that Requirement R2.1 The Cyber Asset uses a routable protocol or Be change to: R2.1 The Cyber Asset uses a routable protocol that is in fact routed over a Wide Area Network (WAN) or;	R2.1 has been modified. Routable protocols has been clarified in the FAQs.
002-R3		

CIP-002 Drafting Team Responses to Comments

002-R4	National Grid recommends changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>	Option for delegate(s) has been added.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-C1,1		
002-C1,2	Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?	Compliance 1.2 has been modified to "Annually". Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Gary Campbell
Entity Name	MAIN

	Comments	*Responses*
General	In levels of compliance, I am assesing non-cpomliance for a 30 day window but have stated it is required.	Not sure what you mean. Time frames mentioned in the Levels of Non_compliance are 90 days and one calendar year.
002-R1		
002-R2		
002-R3		
002-R4		
002-M1	M1 - The measures should not be referencing the requirements such as " as identified in R1". The requirement should contain all the components to be measured. In M1, in could read the " the Respnsoble Entity shall maintian the list of Critical Assets"	The requirements and measures have been modified.
002-M2	M2 - Do not any requiremetns for measure nor is it mention that it must be used.	The requirements and measures have been modified.
002-M3	M3 - Is confusing in that I am not sure if I am suppose to maintain a list of other Critcal Assts only and do not have to maintain a list for anything else.	The requirements and measures have been modified.
002-M4	M4 This should be part of requirements and the measure should be that we look for the updates.	The requirements and measures have been modified.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Gordon Pietsch
Entity Name	Great River Energy

Comments		*Responses*
General		
002-R1	Requirement R1.1.6 states that "Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration" must be included in an organization's list of Critical Assets. It is not clear what the scope of "initial system restoration" includes, and therefore is unclear which substation and transmission lines are to be included. Does this apply only to the substations and lines that directly support a Blackstart generator and are within a certain proximity? Or does it include all subs and lines used in cranking paths to baseload generators? Or is the scope limited in terms of time (i.e., does "initial" mean the first 1 or 2 or 3 days of restoration)?	R1.1.6 has been modified.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Greg Mason
Entity Name	Dynegy Generation

	Comments	*Responses*
General		
002-R1	Section R.1.1.6 defines all Blackstart generators(regardless of size) as Critical Assets.Analogous to Sections R.1.1.4 and R.1.1.5,we recommend that a size limitation be established whereby all Blackstart generators below the specified size limitation are not defined as Critical Assets.One option would be to base the size limitation on a net MW output level.If this approach is adopted,we suggest 25 MW be established as this size limitation.A second option would be to base the size limitation on a % of the total blackstart capability within a Reliability Region or ISO.If this approach is used,the Reliability Region or ISO would need to be involved in setting this percentage.	All generators identified as Blackstart generators regardless of size are required to be protected and secured as per the Cyber Security Standards.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Guy Zito
Entity Name	NPCC CP9

	Comments	***Responses***
General	CIP-002 is not ready for ballot. It is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. NPCC Participating Members suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.>>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. Cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed.
002-R2		
002-R3		
002-R4	Change Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>	Option for delegate(s) has been added.
002-M1		

CIP-002 Drafting Team Responses to Comments

002-M2

002-M3

002-M4

CIP-002 Drafting Team Responses to Comments

002-M5	Change Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-M6	Change Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-C1,1		
002-C1,2	Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Howard Rulf
Entity Name	We Energies

Comments		*Responses*
General		
002-R1	Remove R1.1.9. You cover this with R1.1.1-8. Change reporting period for asset changes from 30 days to 90 days. Clarify weather senior manager needs to sign offon changes to assets. Because this standard has been expanded to include control areas in generating stations and transmission substations, the senior manager responsible will more than likely be multiple people, based on business area. This should be reflected in all parts of the standard. Why identify critical assets and manage them if they are not cyber and subject to this standard?	The SAR requires that Responsible Entities use a risk-based assessment to identify Critical Assets. Lists must be updated within ninety calendar days of the addition of, removal of, or modification. Option for a delegate(s) has been added. Critical Assets must be identified to ensure additions or modifications comply with the Cyber Security
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	James W. Sample
Entity Name	California ISO

	Comments	*Responses*
General	Purpose:The words “would adversely impact” should be changed to “would significantly impact”. Compliance Measures: Suggest this section refer to a “significant or material change” and should be 90 days. This section (in several areas) refers to “officers” whereas the other standards refer to “senior manager”. We recommend a standard term of “senior manager or designee”.	The purpose of CIP-002 has been modified. The lists must be updated within ninety calendar days of the addition of, removal of, or modification. A senior manager or delegate(s) replaces previously referred to officers.
002-R1	Suggest removal of R 1.2 – R 1.10 o the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Jerry Freese
Entity Name	American Electric Power

	Comments	*Responses*
General	In general, we believe that the measures should line up with the requirements. For both compliance and levels of non-compliance, standardize on quarterly for every review cycle. So, "verify annually that changes are made quarterly."	The measures have been revised to match the requirements.
002-R1	R1 should end with a colon instead of a period. The purpose of restating R1 in R1.1 as well as the definition of a Critical Asset is not immediately clear. If the definition must remain in the requirement text, it should be consistent with the official definition given at the beginning of the standard (i.e., should contain no additional verbiage). We believe that R1.1 should be eliminated and the "level 3" requirements should be promoted to "level 2"	R1 has been modified. Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System.
002-R2	In R2, "critical Cyber Assets" should be "Critical Cyber Assets" (with a capital "C") In R2.3, we disagree with this statement. Dialing up to a terminal server doesn't necessarily involve routable protocols, but the remote device may very well have point-to-point connections (i.e. serial) to multiple Critical Cyber Assets. These devices should still be given a physical perimeter. Maybe not the same Physical Security Perimeter found at a control center, but a physical security perimeter nonetheless. Otherwise, this is going to cut down on physical protection of Critical Cyber Assets.	R2.3 has been removed.
002-R3	In R3, add "as though they are Critical Cyber Assets" after "must be protected" to require all assets on a critical segment to be protected equally.	R3 has been removed.
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		

CIP-002 Drafting Team Responses to Comments

002-C2,2

002-C2,3

002-C2,4

The compliance section has been modified.

CIP-002 Drafting Team Responses to Comments

Commentor	Jerry Heeren
Entity Name	MEAG Power

	Comments	***Responses***
General	A3 and R1.1 - The term “bulk electric system” needs to be capitalized in R1.1, and defined on the Definitions of Terms page. A definition of this term is suggested at the top of this document.	The Bulk Electric System is defined in the NERC Glossary of Terms.
	Other Comments -- Requirements and Measures numbering scheme does not match.	The measures have been revised to match the requirements.
002-R1	A3 and R1.1 - The term “bulk electric system” needs to be capitalized in R1.1, and defined on the Definitions of Terms page. A definition of this term is suggested at the top of this document.	The Bulk Electric System is defined in the NERC Glossary of Terms.
	Each of the eight Cyber Security Standards, including this CIP-002-1, begins with a page of definitions. One of the defined terms is Critical Asset. Yet within CIP-002-1, requirement R1.1 presents a significantly different definition of Critical Assets. The definition at R1.1 lists specific items that are not on the Definition of Terms page. But the R1.1 definition also omits concepts that are on the Definition of Terms page (for example, time, heath, and safety). Why are two different definitions needed? This ambiguity makes it difficult for smaller utilities to determine whether CIP-003 through CIP-009 apply.	R1 has been modified.
	R1.1's definition of Critical Assets uses two terms: "the electric grid" and "the interconnected bulk electric system." While the Cyber Security FAQ's Venn diagram does depict the "Bulk Electric System," it does not show "the electric grid." We believe that there are portions of the electric grid that lie outside the bulk electric system. We do not believe this standard was intended to apply to all of the electric grid, including for example our 46 kV and 69kV assets. Unless this definition is clarified, we will decide for ourselves which portions of our electirc grid (>200 kV) comprise the bulk transmission system when we perform our risk-based assessment.	
	We own but do not directly operate any Bulk Electric System generation or transmission facilities. We are joint owners of assets that are operated by another owner. Thus, we recommend that the last sentence in R1.1 be changed to read: "Those Critical Assets may include the following:"	
	R1.1.4 and R1.1.5 use 80% of the Region's largest single contingency as a threshold for defining critical generation assets. Yet R1.1.7 uses 300 MW as the threshold for defining automatic load shed systems as critical assets. In our Region, the difference between the generation threshold and the load shed system threshold is greater than 500 MW. This means relatively small generators are NOT considered critical to reliability, but the same magnitude of load shed capability IS critical to reliability. Why use such different thresholds? We suggest changing the 300 MW used under R1.1.7 to the same 80% standard of largest single contingency as is used in R1.1.4 and R1.1.5.	
002-R2	R2.1 -- The term “routable protocol” needs to be defined and clarified further. Does routable protocol include TCP/IP and DNP 3.0 only -- or are there other routable protocols? Also, is the R2.1 requirement removed if a “routable protocol” (as it is defined) is encrypted?	R2.1 has been modified. Routable protocols has been clarified in the FAQs.
002-R3		

CIP-002 Drafting Team Responses to Comments

CIP-002 Drafting Team Responses to Comments

Commentor	Jim Hansen
Entity Name	Seattle City Light

	Comments	*Responses*
General	Compliance should be numbered in the same fashion as Requirementss (Rn) and Measures (Mn). example: R1.1, M1, C1.1.2. This would make it easier to refer to particular sections of the standard from documents and programs we develop for compliance. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example in CIP-005 M1 -- 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'.	The measures have been revised to match the requirements.
002-R1	R1.1.1: The word 'performing' in the first sentence might be interpreted to mean 'actively performing'. This generally does not apply to backup control centers. If applied litterally, then backup control centers would not fall under this requirement unless they were actively performing one of the critical functions listed here. We believe the intent is to monitor these facilities 7x24 whether they are active or not. We suggest that the wording be changed to 'Control centers and backup control centers that, when operational, perform the functions of -' R1.1.2: The use of the phrase 'such as', in this section, when taken together with the last sentence of R1.1 causes us some confusion. Do the authors intend to allow Responsible Entities to apply their risk-based assessment to identify which of these functions are critical to the operation of the control centers or is this a perscriptive list? If the latter, then the phrase 'such as' should be changed to 'shall include'. If not, then the phrase should be changed to 'for example' and it should be made clear that systems performing certain of these functions may not be critical to the operation of the control center. For example, control centers that are not transmission service providers may not need to include cyber assets running real-time power system modelling. Also, depending on the type of data being exchanged, inclusion of inter-utility data exchange may not be appropriate. R1 and R2: It would helpful if a flow chart were provided that would provide the industry with a consistent approach to applying R1 and R2 R1.1.3: The phrase associated with in the first sentence extends beyond equipment within the IROL transfer path. This requirement should state that anything not in the direct transfer path is excluded. Responsible Entities applying their risk-based assessment would identify anything outside the path that might impact the transfer path. R1.1.7 Please tie the requirement to a specific criteria rather than 300 MW.	Your stated intepretation is correct and applies to all backup functions and facilities.
002-R2	R1 and R2: It would helpful if a flow chart were provided that would provide the industry with a consistent approach to applying R1 and R2 R2: A clarification was made during the conference call, and later confirmed during our WECC EMSWG meeting, that Cyber Assets using a routable protocol would not be considered Critical Cyber Assets if	A flowchart has not been provided as the process is dependent on Responsible Entity's organization and available skills. Critical Cyber Assets with dial-up access must be protected under the Cyber Security Standards.

	these assets were electronically isolated. In other words, there were no routable or dial-up electronic access points to the system. The requirements in this section do not state this however. The requirements need to be clarified to include this point. We suggest modifying R2.1 to state: The Cyber Asset uses a routable protocol for access from outside the electronic security perimeter. This will exclude power plants and substations that use a network of Cyber Assets to provide governor control, data acquisition, etc. but are connected outside their electronic perimeter by RTU protocol communications only. It would also exclude Cyber Assets in control centers and backup control centers that have no external electronic perimeter access points using a routable protocol or dial-up modem.	See CIP-005 for clarification on non-routable protocols
002-R3		
002-R4	R4 Please clarify that senior management are not required to sign a detailed list of Critical Assets and Critical Cyber Assets. For example, we should be able to identify our control center and EMS system as critical assets and cyber assets respectively without providing management with a detailed list of all of the critical equipment in each.	Option for delegate(s) has been added.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	M5-6 should require annual review by senior staff. Signature and review on change would usually require daily or weekly review.	Annual review by senior a manager or delegate(s) has been added.
002-M6	M5-6 should require annual review by senior staff. Signature and review on change would usually require daily or weekly review.	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Jim Hiebert
Entity Name	California ISO

	Comments	***Responses***
General	Compliance should be numbered in the same fashion as Requirementss (Rn) and Measures (Mn). example: R1.1, M1, C1.1.2. This would make it easier to refer to particular sections of the standard from documents and programs we develop for compliance. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example in CIP-005 M1 -- 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'.	The measures have been revised to match the requirements.
002-R1	R1 and R2: It would helpful if a flow chart were provided that would provide the industry with a consistent approach to applying R1 and R2. R1.1.1: The word 'performing' in the first sentence might be interpreted to mean 'actively performing'. This generally does not apply to backup control centers. If applied litterally, then backup control centers would not fall under this requirement unless they were actively performing one of the critical functions listed here. We believe the intent is to monitor these facilities 7x24 whether they are active or not. We suggest that the wording be changed to 'Control centers and backup control centers that, when operational, perform the functions of -' R1.1.2: The use of the phrase 'such as', in this section, when taken together with the last sentence of R1.1 causes us some confusion. Do the authors intend to allow Responsible Entities to apply their risk-based assessment to identify which of these functions are critical to the operation of the control centers or is this a perscriptive list? If the latter, then the phrase 'such as' should be changed to 'shall include'. If not, then the phrase should be changed to 'for example' and it should be made clear that systems performing certain of these functions may not be critical to the operation of the control center. For example, control centers that are not transmission service providers may not need to include cyber assets running real-time power system modelling. Also, depending on the type of data being exchanged, inclusion of inter-utility data exchange may not be appropriate. R1.1.3: The phrase associated with in the first sentence extends beyond equipment within the IROL transfer path. This requirement should state that anything not in the direct transfer path is excluded. Responsible Entities applying their risk-based assessment would identify anything outside the path that might impact the transfer path. R1.1.7 Please tie the requirement to a specific criteria rather than 300 MW.	A flowchart has not been provided as the process is dependent on Responsible Entity's organization and available skills. Your stated intepretation is correct and applies to all backup functions and facilities.
002-R2	R2: A clarification was made during the conference call, and later confirmed during our WECC EMSWG meeting, that Cyber Assets using a routable protocol would not be considered Critical Cyber Assets if these assets were electronically isolated. In other words, there were no routable or dial-up electronic access points to the system. The requirements in this section do not state this however. The requirements need to be clarified to include this point. We suggest modifying R2.1 to state: The Cyber	Critical Cyber Assets with dial-up access must be protected under the Cyber Security Standards. The measures have been modified

	Asset uses a routable protocol for access from outside the electronic security perimeter. This will exclude power plants and substations that use a network of Cyber Assets to provide governor control, data. acquisition, etc. but are connected outside their electronic perimeter by RTU protocol communications only. It would also exclude Cyber Assets in control centers and backup control centers that have no external electronic perimeter access points using a routable protocol or dial-up modem.	
002-R3		
002-R4	R4 Please clarify that senior management are not required to sign a detailed list of Critical Assets and Critical Cyber Assets. For example, we should be able to identify our control center and EMS system as critical assets and cyber assets respectively without providing management with a detailed list of all of the critical equipment in each.	Option for delegate(s) has been added.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	M5-6 should require annual review by senior staff. Signature and review on change would usually require daily or weekly review.	Annual review by a senior manager or delegate(s) has been added.
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Joe Weiss
Entity Name	KEMA

	Comments	***Responses***
General	Business and operational demands for managing and maintaining a reliable electric system increasingly require Cyber Assets supporting critical reliability control and diagnostic functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical electric system assets. This standard requires that Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the electric system. The Critical Assets are identified by the application of Critical Asset cyber risk-based assessment procedure on the operation of the electric system. FAQ 2. Critical Cyber Assets using non-routable protocols could have a range of potential cyber impacts and should be assessed using a risk-based approach. FAQ 3. This addresses common mode failure within the power plants. However, many large and small power plants are now electronically interconnected to the bulk electric system for real time dispatch and other real-time functions. That means that the power plants, however small, can be an insecure electronic path into the bulk electric grid and control center. Consequently, a risk-based approach should be used to determine if they should be included in this standard. FAQ 8. A continuously connected dial-up, if interrupted, becomes non-permanent communication connection as it will need to be reconnected at which time it could become vulnerable. FAQ 12. Since cyber impacts on communication systems have already impacted Critical Cyber Assets, a risk-based approach should be used to evaluate communication systems between Electronic Security perimeters and Critical Cyber Assets. The risk-based approach would identify if the communications need to be addressed and to what level. FAQ 13. The exception would be if there is electronic interconnectivity between the environmental or support system and the Critical Cyber Asset. If there is electronic connectivity, then the environmental or support system should meet the same criteria as the Critical Cyber Asset.	The purpose of CIP-002 has been modified. Electronic Security Perimeters are required to protect Critical Cyber Assets from other Cyber Assets. The Responsible Entity must identify specific risk-based assessment criteria.
002-R1	R1.1 Critical Assets: The Responsible Entity shall... critical operating functions and tasks affecting the interconnected electric system ...power plant control and diagnostics, substation control and diagnostics and real time information exchange... This criteria was not based on cyber considerations. Even small units that are cyber vulnerable and electronically connected to a control center can impact the control center and associated bulk electric grid. Additionally, packages of small combustion turbine units that individually would be considered too small to individually address can constitute a large station. Each small unit could be cyber vulnerable. Having	Electronic Security Perimeters are required to protect Critical Cyber Assets from other Cyber Assets.

	the standard ignore these units can contribute to the electronic vulnerability of the bulk electric grid.	
002-R2	R.2.1. A risk-based graded approach should be used to determine the applicability of all Critical Cyber Assets whether using a routable or non-routable communication protocol. Communication protocols such as DNP3, Modbus, and Profibus currently can be (and in many instances have been) accessed to make the Critical Asset vulnerable. The cyber vulnerability of control system non-routable protocols have been demonstrated in laboratory demonstrations such as the DOE Pacific Northwest National Laboratory (PNNL) demonstrations and in field cases resulting in actual (though not publicly reported) control system cyber impacts. Non-routable control system communication protocols have actually actual caused cyber impacts. Consequently, there is a need for a graded risk-based approach to determine the impact of the Asset independent of the protocol. If they cannot impact the bulk electric grid, they do not need to be addressed. If they can impact the bulk electric grid, the risk-based approach should provide a basis for the level of protection. R.2.3. Delete.	The Responsible Entity could identify, if desired, non-routable communication protocols in their risk-based assessment.
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	John Lim
Entity Name	Con Edison

	Comments	***Responses***
General		
002-R1	R1: the word "preferred" in "Responsible Entities shall identify their critical Assets using their preferred risk-based assessment." might leave things too open for different interpretations. Either replace with another word (determined??) and/or give more guidance.	R1 has been modified.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Karl Tammer
Entity Name	ISO/RTO Council

	Comments	*Responses*
General	Purpose: The words "would adversely impact" should be changed to "would significantly impact".	The purpose of CIP-002 has been modified.
002-R1	Suggest removal of R 1.2 -- R 1.10 o the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The measures have been revised to match the requirements.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	Suggest this section refer to a "significant or material change" and should be 90 days.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-M5	This section (in several areas) refers to "officers" whereas the other standards refer to "senior manager". We recommend a standard term of "senior manager or designee".	Annual review by sa enior manager or delegate(s) has been added.
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Kathleen M. Goodman
Entity Name	ISO New England Inc.

	Comments	***Responses***
General	The standard does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exists regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed. Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.ISO-NE believes that CIP-002 is not ready for ballot. We believe it is important that it is clarified that the Critical Assets specifically identified are a subset of the Critical Assets as defined in the Definitions section. In the purpose, the words <<would adversely impact>> should be changed to <<would significantly impact>>. In MEASURES, This section (in several areas) refers to <<officers>> whereas the other standards refer to <<senior manager>>. We recommend a standard term of <<senior manager or designee>>.Suggest MEASURES refer to a <<significant or material change>>. Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200	R3 clarifies the requirements for a Responsible Entity with no Critical Assets or no Critical Cyber Assets. Annual review by senior manager or delegate(s) has been added. References to unattended facilities have been removed. The purpose of CIP-002 has been modified.
002-R1	Suggest removal of R 1.2 - R 1.10 to the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section.We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed. Annual review by senior manager or delegate(s) has been added.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	M4 should be 90 days.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.

CIP-002 Drafting Team Responses to Comments

002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Keith Fowler
Entity Name	LG&E Energy Corp.

	Comments	*Responses*
General	We are in agreement with the comments submitted by the ECAR CIPP group.	Please see responses to ECAR CIPP group.
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Ken Fell
Entity Name	New York Independent System Operator

	Comments	*Responses*
General	Modify requirement for approval or signature from “senior management” to allow for senior management designee.	Option for a delegate(s) has been added.
002-R1	Migrate Requirements R1.2-R1.10 to faq section, allowing appropriate Risk Based Assessment to identify critical assets.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	Change Measure M4 to require documentation for “significant or material change” of cyber assets, in place of the existing “addition of, removal of, or modification to.” Allow for 90 day time frame to reflect said change.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Kurt Muehlbauer
Entity Name	Exelon Corporation

	Comments	*Responses*
General	Please provide more direction, perhaps in a FAQ, on whether voice and PBX telecommunications equipment should be considered in the risk-based assessment. Or should they be considered support systems as described in FAQ 13?	Under Applicability 4.2.2 communciation networks and data communciation links between Electronic Security Perimeters are exempt from this standard. PBX telecommunications relies on communication networks. All communications could be considered support systems as described in FAQ 13.
002-R1		
002-R2		
002-R3	We believe that the risk-based assessment and applying greater protections to Critical Cyber Assets is a sound security practice introduced in this standard. However, R3 and M3 could be interpreted that all assets within the perimeter are subject to the CIP-002 through CIP-009 standards. If this interpretation is correct, it could result in non-critical assets being added to the scope of these standards and negate the benefits of the risk-based assessment. The purpose of R3 should be to identify other assets that are within the same Electronic Security Perimeter as identified Critical Cyber Assets. R3 should not define protection mechanisms. We recommend that R3 be changed to: The responsible entity shall identify other Cyber Assets within the same Electronic Security Perimeter as the identified Critical Cyber Assets.	R3 has been removed.
002-R4		
002-M1		
002-M2		
002-M3	In M3 the sentence reads: …Critical Cyber Assets as identified under Requirement R3… Critical Cyber assets are identified in R2, so the sentence should be changed to: …Critical Cyber Assets asssts identified under Requirement R2…	The measures hve been modified.
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	L.W. Brown
Entity Name	Edison Electric Institute

	Comments	***Responses***
General		
002-R1	R1. The opening sentence indicates that each Responsible Entity may use their preferred risk assessment methodology to identify Critical Assets. However, the Requirement then proceeds to include a very specific list of facilities (R1.1.1 - R1.1.8). The impression is given that such list would override any entity's own risk assessment. It would be better if the standard only include R1.1 and R1.1.1 (renumbered as "R1.2"). The listed facilities should either be moved to the FAQ, or – if the FAQ is not included – more clearly identified only as facilities that are likely to critical and so must be included within an assessment, but which may – after such an assessment – be found reasonably excludable. Such a revision would require either removing the last sentence of the current R1.1, or (if the current list at R1.1.1 - R1.1.8 is retained) inserting the word "may" or "could" prior to the word "include" in that sentence. R1.1.1. Use of the term "Generation Operator" in R1.1.1 implies that all generation equipment is covered by the standard. It had been the understanding of most companies that generation facilities were not to be covered in all cases.	R1 has been modified.
002-R2		
002-R3		
002-R4	R4. The term "senior management" is unclear. Does this mean the "senior management officer" mentioned in CIP-002-1 Measure M5, or the officer or senior management official responsible for the cybersecurity policy under CIP-003?	Annual review by a senior manager or delegate(s) has been added. The senior manager or delegate(s) in various standards could be different individuals as appropriate for the Responsible Entity.
002-M1		
002-M2		
002-M3	M3. Reference is made to R3 – that appears to be typo, as the identification of Critical Cyber Assets is in R2.	The measures have been modified.
002-M4		
002-M5	M5. Must the record of approval of the list be updated for every individual change to that list? If so, we urge reconsideration, as that is far too burdensome.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification. Option for delegate(s) has been added.
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity Name	ECAR Critical Infrastructure Protection Panel

	Comments	***Responses***
General		
002-R1	R.1.1.1. Change Control Centers to System Control Centers R1.1.3. & R1.1.8 -- While a definition exists of an IROL, some additional explanation may be required to ensure common understanding of how these requirements should be applied.	Control centres can refer to Regional or Balancing Authorities (Area) Control Centres. System Control Centres are not defined in the NERC Functional Model.
	R.1.1.4. Change <<Generating resources under control of a common system >> to <<Generating resources under control of a common plant control system>>	R1.1.4 modified.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	Change <<A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained>> to <<A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained annually.>>	The measures have been modified. Annual review by a senior manager or delegate(s) has been added.
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity Name	Cinergy

	Comments	***Responses***
General		
002-R1	CIP-002-1 B.R1.1.3 & R1.1.8.--IROL: While a definition exists of an IROL, some additional explanation is required to ensure common understanding of how these requirements should be applied.	IROL is defined in the NERC Glossary of Terms.
002-R2	R.2.1.Cyber assets that use a routable protocol: Because cyber assets, which use a routable protocol, must be protected both physically and electronically, in effect, entities which move to a routable protocol are penalized. We believe this type of requirement will impede progress toward routable protocols in substations. The level of administrative and cost burden may cause Cinergy and other companies to delay or avoid moving to routable protocols and, therefore, they will continue to operate with less information and less reliability. We urge NERC to reconsider requiring the physical perimeter if a routable protocol is used.	R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the
002-R3		
002-R4	R.4. Member of senior management must approve the list of critical assets. This is an un-necessary level of approval. The senior management's name(s) are included in the policy. It is not necessary for the senior management to approve individual lists, etc. These types of requirements add administrative burden with no offsetting enhancement in security.	This requirement has been modified.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Laurent Webber
Entity Name	Western Area Power Administration

	Comments	***Responses***
General	Purpose: The term (critical reliability control functions) is not well defined both in the sense of what is critical and what are the "reliability control functions". R1.1.2, R1.1.7, R2.1, R2.2, and R3 seem to require that Critical Assets be defined down to the component level. This, combined with the requirements and measures listed in this and other CIPs (i.e. CIP-003-R3, CIP-005-M1 CIP-004-M3, CIP-004-M4, CIP-004-4.3, CIP-004-M4.4, CIP-005-R5, CIP-006, CIP-007-R5, CIP-009) creates a cascading requirement that would lead to huge lists of every device and result in an undue burden of documentation, testing, and tracking of individual Intelligent Electronic Devices (IEDs). It must be made clear that the listing of critical assets and critical cyber assets does not extend down to the component level.	The purpose of CIP-002 has been modified. Critical Cyber Assets perform critical operating functions or tasks which could include IEDs.
002-R1	WAPA suggests that R1.1 be revised to include the sentence, (Critical assets, critical cyber assets, and associated risk-based assessments, security plans and lists may be identified at a system level rather than a component level.) R1.1.3 and R1.1.8 create a cascading effect with the requirement to include (elements monitored as…IROL) and (elements associated with an IROL.) These would be better worded as: [R1.1.3. Transmission substations in the direct electrical path of elements monitored as Interconnection Reliability Operating Limits (IROL)] and [R1.1.8. Special Protection Systems protecting elements monitored as IROL.] R1.1.5 would include generating resources of about 2000 MW, and R1.1.7 includes load shedding of 300 MW. This seems to be a wide discrepancy in the amount of electrical power defined as critical. R1.1.6 creates a cascading effect with the requirement to include (substations associated with transmission lines used for initial system restoration.) It would be better worded, (substations in the electrical path of transmission lines used for initial system restoration.)	R1 has been modified.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		

CIP-002 Drafting Team Responses to Comments

CIP-002 Drafting Team Responses to Comments

Commentor Lawrence R Larson, PE

Entity Name Midwest Reliability Organization

	Comments	*Responses*
General	For Applicability (Section 4) of all the CIP(s), Nuclear facilities are exempted. The way this is phrased causes concern, because these facilities impact the grid just as other generators do. Does the NRC assure that nuclear facilities meet or exceed these cyber security standards? If so, that should be stated. If not, additional information about safeguards that do apply to these facilities should be provided.	Under Applicability 4.2.1 has been modified to exempt only the facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
002-R1	While it indicates that an appropriate risk assessment methodology should be applied, it then also goes on to provide too much prescriptive detail about what has to be inside and outside that risk assessment. It is not up to the Standard drafting team to define what the critical assets are; each company should identify them based on their risk assessment. Much of the language under R1.1.1 - R1.1.9 should be eliminated, and the simple instructions that an appropriate assessment methodology should be developed and used should be left to stand on its own. R1.1.3 and R1.1.8 are particularly problematic. Each entity should define how they will assess risk for elements outside the control center (substations, etc), and should be able to demonstrate that they are abiding by that assessment - R1.1.3 to R1.1.9 inappropriately force particular outcomes (e.g. inappropriatly requires that many substations become Critical Assets). The words DETRIMENTAL IMPACT in section R1.1 are problematic, because it would be definined diferently by different entities.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		

CIP-002 Drafting Team Responses to Comments

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Lee Matuszczak
Entity Name	U S Bureau of Reclamation

	Comments	*Responses*
General		
002-R1	Is it appropriate that critical non-cyber asset identification, included in this list, should fall under this standard? It would appear that NERC should address non-IT critical infrastructure under a separate identification and protection standard and then supplement that standard with the cyber security standard. R1.11 - Is it appropriate for entities to conduct these risk-based assessments in isolation? To be effective, such assessments may be more useful if addressed from the perspective of the NERC Region or from from the standpoint of their significance to the overall "power grid". Failure to examine and identify critical non-cyber assets at a Regional or Grid level may lead to identification and excessive protection of less significant but "entity business-essential" systems by the entities. While the protection of these assets may be important to the individual entity, they are not the subject of this standard and will divert resources from higher priority and potentially more important assets.	The requirement for a list of non critical cyber assets has been removed.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3	M3. - References to requirements R2 and R3 are included in this section for which no content appears to be present	The standard has been renumbered.
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor Linda Campbell

Entity Name FRCC

	Comments	*Responses*
General	During the conference call conducted for the first draft, we posed a question as to whether a facility that houses critical assets, but has no external connectivity, either dial-up or network, still fell under this standard. The response from the host of the session, Larry Bugh, was that these assets were not covered by this standard. During the Feb 2 conference call there was discussion around standard CIP-002, which implied that this may not be the case. Can the drafting team clearly address facilities that have no external connectivity, but house critical assets that run a routable protocol? The standard does not clearly indicate wheather support systems such as cooling, UPS, generators, etc. that are outside the physical security perimeter should be considered critical assets. If these systems are considered critical assets, then they should be included in the physical security perimeter. The standard must define the outermost boundery of the physical perimeter. . Section Inconsistency remains between levels of non-compliance across standards.... For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006. The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards. 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?	R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the facility. Support systems are not required to be identified as Critical
002-R1	R1.1 must be reworded so as not to regurgitate the definition of a Critical Asset. Critical Asset will be added to the NERC Glossary and will not need to be defined within the standard. R1.1 should be reworded as follows: Critical Assets: The Responsible Entity shall identify its Critical Assets, which consists of, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control, and real-time information exchange. Those Critical Assets including the following: R1.1.1. Should be stricken from the document. There is no need to duplicate the list of applicable functions as already listed the introduction's section 4. Applicability. Removing redundant information will ensure swift compliance and clearly delineate compliance measurements. R1.1.9. Should be stricken from the document. R1.1.1 through R1.1.8. are just examples used to clarify	R1 has been modified.

	the types of areas the Responsible Entity has to assess in order to fully comply with requirement R1. There is no further need to reiterate requirement R1.	
002-R2	The words “for the purpose of this standard” have no value when in a sentence with a proposed NERC term. Upon approval of this standard the definition of a Critical Cyber Asset will be added to the NERC Glossary, once approved, all NERC standards that use the term “Critical Cyber Asset” will need to follow the NERC definition. If this sentence is left in the standard, then NERC will be setting precedence that NERC terms can be superseded within any individual standard. The appropriate way to handle this issue is to change the definition of a “Critical Cyber Asset” to incorporate the requirements of R2.	The purpose of CIP-002 has been modified.
002-R3	R3. needs to be re-worded, the words "as identified" were already used in R1. and therefore can allow for a conflicting interpretation of how to determine the applicability of this requirement. R3. should be re-worded as follows: Any other Cyber Asset within the same Electronic Security Perimeter of Critical Cyber Assets must be protected as if a Critical Cyber Asset itself.	This requirement has been removed.
002-R4		
002-M1		
002-M2		
002-M3	M3. has a typo, the first instance of Requirement R3 should be R2. The corrected sentence would be: M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3.	The measures have been modified.
002-M4		
002-M5		
002-M6		

CIP-002 Drafting Team Responses to Comments

002-C1,1		
002-C1,2		
002-C1,3	D1.1.2. should be reworded to conform to the Compliance sections. Proposed language would be: D1.1.2. Compliance Monitoring Period and Reset Timeframe. 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.The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. R2. should be re-worded as follows: R2. The Responsible Entity shall identify the Critical Cyber Assets associated with each Critical Asset	The Compliance Section has been modified.
002-C1,4	listed in section R1.	
002-C2,1	The definition of “Critical Cyber Asset” should be changed to:	
002-C2,2		
002-C2,3	Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets having the following characteristics: 1. The Cyber Asset uses a routable protocol, or	
002-C2,4	2. The Cyber Asset is dial-up accessible. 3.-- Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter.	

CIP-002 Drafting Team Responses to Comments

Commentor	Lyman Shaffer
Entity Name	Pacific Gas and Electric Company

	Comments	***Responses***
General	Introduction/Purpose: In the second paragraph of the introduction it reads ", where loss or compromise of these assets..." it should read ", where loss of availability or compromise of the integrity of these assets...".	The purpose of CIP-002 has been modified.
002-R1	R1.1 unclear whether the intent of this is to be proscriptive or just listing examples" R1.1.2 appears that critical cyber assets are listed as critical assets themselves -- suggest striking the text 'such as .....inter-utility data exchange' R1.1.1 -- change "performing" to "with" to read: "...backup control centers with the functions of...". R1.1.3 -- This requirement should state that it excludes anything not in the direct transfer path associated with the IROL. R1.1.7 -- Shouldn't the load shedding requirements refer to the reporting requirements imposed operating standards versus the prescriptive 300 MW. Tie it to reporting criteria.	R1 has been modified. R1.1.2 has been modified. R1.1.1 was nort modified as suggested. R1.1.3 has been modified. R1.1.7 see FAQ 5. See FAQ 5 for clarification of the 300 MW load shedding requirement.
002-R2	R2 We are looking for more clarification regarding this requirement due to mixed messages from the working, the NERC 1300 Web cast, and discussions with drafting team members. If a control center and a plant have routable protocols within each of their electronic perimeters, but have no routable protocols through their electronic perimeter are both or either subject to the electronic requirements of this standard? Understanding that both are subject to the physical security requirements of this standard.	R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the
002-R3		
002-R4	R4. Due to the update frequency of a detailed list, this requirement should be wording in a manner that will only require senior management to sign off on functions/systems and not the detailed components of these functions/systems. The detailed list is required to be keep up to date by an operational unit.	Annual review by senior manager or delegate(s) has been added.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	M5 & M6 -- These measures refers to "Officers" and is not consistent with all other references to "Senior Management". These measures should also include time frames like all the other measurements (e.g. M4). Suggest a measurement of an annual review.	Annual review by a senior manager or delegate(s) has been added.
002-M6	M5 & M6 -- These measures refers to "Officers" and is not consistent with all other references to "Senior Management". These measures should also include time frames like all the other measurements (e.g. M4). Suggest a measurement of an annual review.	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		

CIP-002 Drafting Team Responses to Comments

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

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

	Comments	*Responses*
General		
002-R1	R1.1.4 What is the definition of the "largest single contingency within the Regional Reliability Organization" as it relates to generation and how is it determined?	The largest single contingency is available from the Regional Reliability Organization.
002-R2	R2. Consider adding a requirement that states the cyber asset must be controllable. If the asset uses a routable protocol or dial-up modem for data gathering purposes only, and it is not possible to initiate any change to the device, then it should be out of scope. Pg 4, R2.1, Regarding routable protocol: from the Comments & Responses document (p 446) it is clear that the drafting team wants frame relay included as a routable protocol and that frame relay access devices (FRAD's) therefore would be part of the electronic perimeter. This is a huge deal in that many substations would be added to the perimeter.	Monitoring can be part of the control process (see FAQ 12).
002-R3		
002-R4		
002-M1		
002-M2		
002-M3	M3 The first instance of the term "Requirement R3" should be "Requirement R2"	The requirements have been modified.
002-M4	In Measure 4 --The term modification should be defined --does the replacement of a keyboard, mouse, or even hard-drive constitute a modification. In Measure 4 --The term addition should be defined --does the connection of any new hardware inside a security perimeter constitute an addition even if the associated application software system has not been loaded at that point or is it the production use of the new cyber asset that constitutes an addition? This would not normally be an issue except the measure has a timing requirement associated with it that implies the starting of a clock to non-compliance if documentation is not updated. In Measure 4 --The measurement refers only to modification of a Critical Asset or Critical Cyber Asset. What about the other Cyber Assets in the same Security perimeter per R3? It would seem that they would be subject to the same review and documentation per the risk they pose to the Critical Cyber Assets or why have R3 at all?	Modifications to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset. Additions to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

CIP-002 Drafting Team Responses to Comments

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Neil Phinney
Entity Name	GSOC

	Comments	*Responses*
General	No. The internal inconsistencies of the definition of Critical Cyber assets make it impractical to vote on at this time. We believe that the issue of the arbitrary criteria of the use of a routable protocol has been partially hidden by the inconsistent definitions of Critical Cyber Assets. We believe that it is a central issue of the document and that a ballot is inappropriate until a thorough discussion of this issue takes place. Requiring a substantially higher level of documentation and audit for systems using advanced protocols discourages system modernization and will lead to a delay in making more data and control available to system operators. Hence these standards which are intended to make our systems more secure may have the opposite effect.	See FAQ 2. R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Patrick Miller
Entity Name	PacifiCorp

	Comments	*Responses*
General	For section B, the requirements are listed as R1.1 through R1.17. This is inconsistent with the outline format. Assuming that all requirements are not subsets of the first, they should be R1 through R17 instead.	The formatting has been corrected.
002-R1		
002-R2	R 2.3 It makes no sense to remove the requirement for a physical security perimeter around a critical cyber asset simply because it does not use a routable protocol to communicate with other assets. What about substations with only dial up access? Do they not need a physical perimeter?	R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the
002-R3		
002-R4	Our organization has critical cyber assets in Generation, Transmission and IT. This entry implies one senior manager will be responsible for approving the list of critical assets. It would be more flexible if it were 'OK' to have multiple senior mangers approve since these assets reside under multiple senior managers.	Annual review by a senior manager or delegate(s) has been added.
002-M1	For section C, M1 -- it is mentioned "…as identified as in R1" which does not exist (as stated above in ID2), rather R1.1. This should be modified to reflect the true reference.	Formatting has been corrected.
002-M2	For section C, M2 -- it is mentioned "…Critical Assets in R1) which does not exist (as stated above in ID2), rather R1.1. This should be modified to reflect the true reference.	Formatting has been corrected.
002-M3	For the section C, M3 -- it is mentioned "..as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3." Neither R2 nor R3 exist, rather R1.2 and R1.3. This should be modified to reflect the true reference.	Formatting has been corrected.
002-M4	For the section C, M4, within an organization of our size it may be more appropriate to have a 60 or even 90 day window for update.	R4 and M4 have been eliminated.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Paul McClay
Entity Name	Tampa Electric

	Comments	*Responses*
General	The numbering in this section is inconsistent with the other standards.. R1.1, R1.2, etc. versus R1, R2, etc.;M1 references R1 but it should be R1.2;M3 references requirements R2 and R3 which do not appear to exist. During the conference call conducted for the first draft, we posed a question as to whether a facility that houses critical assets, but has no external connectivity, either dial-up or network, still fell under this standard. The response from the host of the session, Larry Bugh, was that these assets were not covered by this standard. During the Feb 2 conference call there was discussion around standard CIP-002, which implied that this may not be the case. Can the drafting team clearly address facilities that have no external connectivity, but house critical assets that run a routable protocol?	The standard has been re-numbered. R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the
002-R1	R1.1.4 No where is “Generating Resources” defined. Is a generating resource a “single generating unit” or a “a combination of units at the same geographical location, i.e. a plant”? This needs to be clarified in the standard. R1.1.9 Calls for a risk based assessment to be conducted by the responsible entity to identify critical cyber assets. Can the organization develop its own risk assessment program? Can the drafting team provide examples of acceptable, industry accepted risk based assessment methodologies? Does the assessment process need to be re-performed annually, or just updated as assets are added/removed?	The generating resource could be a single unit or a combination of units at a plant. FAQ 3 states: "Cyber Assets providing generator local monitoring, local control, or local protection could be a common mode of failure for multiple units. Any such Cyber Asset must be considered a Critical Cyber Asset if the total potential generation affected is equal to or greater than the generation limit in the Cyber Security Standards."
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		

002-C2,2

002-C2,3

002-C2,4

facility.

CIP-002 Drafting Team Responses to Comments

Commentor	Pedro Modia
Entity Name	Florida Power and Light

	Comments	*Responses*
General	The standard does not clearly indicate wheather support systems such as cooling, UPS, generators, etc. that are outside the physical security perimeter should be considered critical assets. If these systems are considered critical assets, then they should be included in the physical security perimeter. The standard must define the outermost boundery of the physical perimeter. Is section 1.3.3 complete, inasmuch as the sentence ends in the word and?	Support systems are not required to be identified as Critical Assets. Section 1.3 has been modified.
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Pete Henderson
Entity Name	Independent Electricity System Operator

	Comments	*Responses*
General	The words “would adversely impact” should be changed to “would significantly impact”.	The purpose of CIP-002 has been modified.
	Renumbering within M3 is required. R2 and R3do not exist.	Formatting has been corrected.
	Compliance Monitoring Process: This section (in several areas) refers to “officers” whereas the other standards refer to “senior manager”. We recommend a standard term of “senior manager or designate”.	The purpose of CIP-002 has been modified.
002-R1	Suggest removal of R 1.2 -- R 1.10 to the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section. The wording of R1.13 appears to apply to programmable logic controllers whether or not they are exposed to the internet or a corporate network. It is not clear that this is either intended or appropriate.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the facility.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	In M4. Suggest this section refer to a “significant or material change” and should be 90 days as per NERC 1200. Furthermore, the specification of a prescribed update frequency is needlessly specific (a risk based approach should be used) and is a requirement and as such, should appear in the “Requirements” section of the Standard.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		

CIP-002 Drafting Team Responses to Comments

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Randy Schimka
Entity Name	San Diego Gas and Electric Co

	Comments	***Responses***
General	Introduction / Purpose - In the second paragraph, the phrase 'loss or compromise of these assets' is used. We suggest that it be changed to something like 'loss of availability or compromise of the asset integrity.' We suggest that matching compliance levels with specific measurements and requirements will help ensure consistent compliance.	The purpose of CIP-002 has been modified. The measures have been revised to match the requirements.
002-R1	Requirements - R1.1 - The phrase 'such as, but not limited to' should be replaced with something like 'shall include, but should not be limited to.' R1.1.3 - Please provide more examples or references about Transmission substations, elements, and IROL. There has been some confusion about how this affects the declaration of certain substation assets as critical cyber assets. R1.1.4 - In WECC, the largest generator is 4,000 MW. So using the 80% criteria presented in this section would mean that a 3,200 MW threshold value would exclude most, if not all, of the generation in our region from having to comply with this standard. It doesn't make sense to apply this Cyber Security standard to our Control Centers and EMS systems and some substation equipment while many generating plants in the region would simply not have to comply. Is this relatively high threshold what was really meant by the drafting team for including (or excluding) generation plants? R1.1.7 - Please identify what the specific criteria is for this section beyond the 300 MW figure that is discussed. Perhaps a flow chart or other visual aid example would be helpful for organizations in applying their situations to R1 and R2.	R1 has been modified. The largest single continency made not be the size of the largest Plant. The drafting team's objective was to exclude the smaller generators while allowing variation based on the Regional requirements.
002-R2	R2 - While providing a simple definition and an easy way to differentiate what should be included in Security efforts vs. not included (routable protocol vs. non-routable protocol), this section or the FAQ would benefit from further definition. Perhaps a flow chart or other visual aid example would be helpful for organizations in applying their situations to R1 and R2.	FAQ 9 has been modified.
002-R3		
002-R4	R4 - This list of critical cyber assets can change periodically, so what is the frequency that the senior management signature is required? We recommend no more frequently than once per year.	Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-M1		
002-M2		
002-M3		
002-M4		

CIP-002 Drafting Team Responses to Comments

002-M5	M5 and M6 - Both of these sections add the word 'officer' to the Senior Management designation. Please define the intent of the approval required. We feel that this would most likely be delegated from the Senior VP down to a Director or Manager level in our organization.	Annual review by a senior manager or delegate(s) has been added.
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

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

	Comments	***Responses***
General	CHGE strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. We suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system. >>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System.
002-R2		
002-R3		
002-R4	We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>	Option for delegate(s) has been added. The measures have been revised to match the requirements.

CIP-002 Drafting Team Responses to Comments

	Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2	Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?	Compliance section 1.2 has been modified. Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Richard Engelbrecht
Entity Name	Rochester Gas and Electric

	Comments	*Responses*
General	NPCC strongly believe that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. We suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.>>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed.
002-R2		
002-R3		
002-R4	We recommend changing Requirement R4 to <<Member(s) of senior management or designee must	R4 has been removed.

	approve the list of Critical Assets and the list of Critical Cyber Assets.>>	
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2	Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?	Compliance section 1.2 has been modified. Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor Richard Kafka

Entity Name Pepco Holdings, Inc. - Affiliates

	Comments	*Responses*
General	R4; M5; M6: This requirement states that a member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. The term “senior management” is unclear. Does this mean the “senior management officer” mentioned in CIP-002-1 Measure M5 & M6, or the "officer or senior management official" responsible for the cyber security policy under CIP-003?	Annual review by senior manager or delegate(s) has been added. The senior manager or delegate(s) in various standards could be different individuals as appropriate for the Responsible Entity.
002-R1	R1: The requirements state that Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. However, the Requirement then proceeds to include a very specific list of Critical Assets (R1.1.1 - R1.1.8). The impression is given that this list overrides an entity’s own risk-based assessment (i.e. if you have these assets then they are Critical Assets no matter what the risk). Is the intent to define these as Critical Assets independent of a risk-based assessment? If yes, R1.1 and R.1.1.9 appear to be the only items that the risk-based assessment applies and this should be clearly stated. If no and R.1.1.1 through R1.1.8 are intended as a list of assets to consider as part of your assessment in identifying Critical Assets then the lead in sentence "Those Critical Assets include the following:" perhaps should be modified to state "Critical Assets may include the following depending on the outcome of a risk-based assessment".	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The Responsible Entity would under "Additional Critical Assets" use the Regional criteria to identify their Critical Assets. R1 has been modified to put the risk-based assessment in R1.2.
	R1: The risk-based assessment appears to only apply to the process of identifying Critical Assets (CIP-002-1, R1) and not Critical Cyber Assets (CIP-002-1, R2) and therefore it is not clearly communicated in the standard that one must use an appropriate assessment methodology to identify critical cyber assets.	
	R1: Further guidance is needed on "using their preferred risk-based assessment". Are there infinite risk-based assessment procedures that a Responsible Entity can choose from or create? If yes would this mean that it is possible that there would be no consistency in identifying Critical Assets and ultimately Critical Cyber Assets across the electric industry?	
	R1: If Critical Assets are defined at one of the ten NERC Area Regional Reliability Councils (e.g. MAAC) for members of that Council (i.e. other Responsible Entities such as Transmission Owners or Generator Owners) does the burden of measures and compliance for R1 fall on the NERC Area Regional Reliability Council rather than the other Responsible Entities?	
	R1.1.6: What T&D assets are included in scope from a blackstart perspective (e.g. generator substation, transmission substations, substations with load)? If a unit has blackstart capability but is not part of the blackstart plan are these assets Critical Assets?	R1.1.6 has been modified. The generation would need to be iidentified in the Blackstart lan to be required by R1.1.6.
002-R2		
002-R3		
002-R4		
002-M1		

CIP-002 Drafting Team Responses to Comments

002-M2		
002-M3	M3. This measure makes reference to R3 as the identification of Critical Cyber Assets. Should this be R2?	The measures have been modified.
002-M4		
002-M5	M5; M6: Are these meant to be annual approvals by the senior management officer or must the senior management officer approve each list for every individual change through out the year? If for every change, could this be reconsidered? Perhaps the senior management officer would approve annually but a delegate would approve through out the year. Even this may be burdensome for M6.	Annual review by a senior manager or delegate(s) has been added.
002-M6	M5; M6: Are these meant to be annual approvals by the senior management officer or must the senior management officer approve each list for every individual change through out the year? If for every change, could this be reconsidered? Perhaps the senior management officer would approve annually but a delegate would approve through out the year. Even this may be burdensome for M6.	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Robert Strauss
Entity Name	New York State Electric & Gas Corporation

	Comments	*Responses*
General	NYSEG concurs with NPCC, that we strongly believe that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section. We suggest the Purpose be altered to <<This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed. With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets. Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.>>	The purpose of CIP-002 has been modified.
002-R1	Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed.
002-R2		
002-R3		
002-R4	We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>	Option for delegate(s) has been added.
002-M1		

CIP-002 Drafting Team Responses to Comments

002-M2		
002-M3		
002-M4		
002-M5	We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-M6	We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>	Option for delegate(s) has been added.
002-C1,1		
002-C1,2	Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?	Compliance 1.2 has been revised. Lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Roger Champagne
Entity Name	Hydro-Québec TransÉnergie

Comments	***Responses***
General	The definition of BES has been removed. The purpose of CIP-002 has been modified.

HQTÉ believes that CIP-002 is not ready for ballot. This is a Cyber Security Standard. A definition of the Bulk Electric System (BES) does not belong in this standard. Recently the industry approved a BES definition, in the Version 0 Glossary. That Glossary was approved so there would be one industry wide definition. NPCCHQTÉ feels that CIP-002 conflicts with that approved definition. We suggest the following Purpose, Requirements, Measures and Compliance.

<<

PURPOSE:

This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, the separation of the critical assets of the bulk electrical system from the an insecure infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require Cyber Assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these Cyber Assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation cyber assets supporting the monitoring and control of the interconnected bulk electric system.

REQUIREMENTS

R1.--The Responsible Entity shall identify their cCritical Cyber Assets associated with support of the bulk electrical system Critical Assets using their preferred risk-based assessment. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics:

R1.1--The Cyber Asset uses a routable protocol, or

R1.2--The Cyber Asset is dial-up accessible.

R1.3--Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter

R2.--Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets.

R3.--A member of senior management or designee must approve the list of Critical Cyber Assets.

MEASURES

M1.--The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R1 and all other Cyber Assets as identified under Requirement R2.

M2.--The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Cyber Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.

M3.--The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, and M2 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset.

M4.--A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.

COMPLIANCE

1.--Compliance Monitoring Process

1.1--Compliance Monitoring Responsibility
Regional Reliability Organization

1.2--Compliance Monitoring Period and Reset Timeframe

Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (l) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.

1.3--Data Retention
The Responsible Entity shall make the following available for inspection by the compliance monitor upon

request:

1.3.1--Documentation of the approved list of Critical Cyber Assets, and

1.3.2-- Documentation of the senior management official's approval of both the Critical Asset list and the Critical Cyber Asset list.

1.4--Additional Compliance Information
Not specified

2.--Levels of Non-Compliance

2.1--Level l:--The required documents exist, but have not been updated with known changes within thirty (30) calendar days.

2.2--Level 2:--The required documents exist, but have not been approved, updated or reviewed in the last calendar year.

2.3--Level 3:--One or more document(s) missing.

2.4--Level 4:--No document(s) exist.
>>

002-R1 ********** Please clarify the performance reset period in D.1.2. What is being reset? Why is it being reset?

002-R2

002-R3

002-R4

002-M1

002-M2

002-M3

002-M4

002-M5

002-M6

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

CIP-002 Drafting Team Responses to Comments

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Roman Carter
Entity Name	Southern Company Generation

	Comments	***Responses***
General		
002-R1	R1.1 What is the definition of the "largest single contingency within the Regional Reliability Organization" as it relates to generation and how is it determined?	The largest single contingency is available from the Regional Reliability Organization.
002-R2	R2 Consider adding a requirement that states the cyber asset must be controllable. If the asset uses a routable protocol or dial-up modem for data gathering purposes only, and it is not possible to initiate any change to the device, then it should be out of scope. Pg 4, R2.1, Regarding routable protocol: from the Comments & Responses document (p 446) it is clear that the drafting team wants frame relay included as a routable protocol and that frame relay access devices (FRAD's) therefore would be part of the electronic perimeter. This is a huge deal in that many substations would be added to the perimeter.	Monitoring can be part of the control process (see FAQ 12).
002-R3		
002-R4		
002-M1		
002-M2		
002-M3	M3 The first instance of the term "Requirement R3" should be "Requirement R2"	The requirements have been revised.
002-M4	In Measure 4 -- The term modification should be defined -- does the replacement of a keyboard, mouse, or even hard-drive constitute a modification. In Measure 4 -- The term addition should be defined -- does the connection of any new hardware inside a security perimeter constitute an addition even if the associated application software system has not been loaded at that point or is it the production use of the new cyber asset that constitutes an addition? This would not normally be an issue except the measure has a timing requirement associated with it that implies the starting of a clock to non-compliance if documentation is not updated. In Measure 4 -- The measurement refers only to modification of a Critical Asset or Critical Cyber Asset. What about the other Cyber Assets in the same Security perimeter per R3? It would seem that they would be subject to the same review and documentation per the risk they pose to the Critical Cyber Assets or why have R3 at all?	Modifications to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset. Additions to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset.
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		

CIP-002 Drafting Team Responses to Comments

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor Scott R Mix

Entity Name KEMA

	Comments	*Responses*
General	Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Identification of Critical Cyber Assets".	The suggestion for changing the title of the standard was not done at the time. Consider resubmitting as comment on draft 3.
	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).	The measures have been revised to match the requirements.
	During the web cast, a question was raised concerning "read-only terminals". It needs to be clear in the requirements and FAQ that any "computer" that is network connected (i.e., on the TCP/IP network) to the control system needs to be protected regardless of the application function used on that computer. This includes PC's and X-terminals that are administratively prohibited from entering data or controls into the control system, but are communicating with the control system. Monitors that are "slaved" to other computers via an RGB or equivalent connection are exempt, since they are not part of the communications (TCP/IP) network, but the computer driving the "controlling" monitor is subject to the requirements of standard CIP-002-1.	FAQ 9 referring to routable protocols has been modfied. Annual review by senior manager or delegate(s) has been added. FAQ 4 referring to IROL has been modified.
	The measures should be re-written as being measurable. For example, M1 should be "The responsible entity shall demonstrate that it has maintained a list of Critical Assets as defined in R1."	
	Measure M5 and M6 should discuss time frames (that are specified in a requirement), i.e., M5 should read "The Responsible entity shall demonstrate that the list of Critical Assets required in R1 has been approved by a senior manager no more than one year after the previous approval, and within one year prior to the audit."	
	FAQ CIP-002-1.Q4 refers to NERC standards in development 200 and 600, which have been adopted by industry and re-named. In addition, out of date definitions are included in the response. Definitions appearing in the NERC glossary should not appear in this FAQ. Definitions not appearing in the NERC glossary should be moved to the Standard text for discussion and adoption by industry.	
	FAQ CIP-002-1.Q7 refers to Token Ring as a layer 3 protocol. IEEE 802.5, which is the international standard for Token Ring, indicates that it is a layer 2 protocol. The reference to "DNP 3.0 (network mode only)" is confusing, and could be interpreted as including all DNP 3.0 traffic. DNP 3.0 is not a layer 3 protocol, nor is it a routing protocol. Replace the term with "DNP 3.0 running over IP" to clarify and limit the applicability.	
002-R1	Requirement R1: Add the following: "The risk assessment process, and the lists of Critical Assets and	R1 has been modified.

	Critical Cyber Assets must be reviewed annually. The lists must be updated within 30 days of the addition of, removal of or modification to any Critical Asset or Critical Cyber Asset.”	
002-R2		
002-R3		
002-R4	Requirement R4 should read: A member of senior management must annually certify that an analysis of the responsible entities’ assets has performed to determine what assets are Critical. If the analysis determines that either no Assets are Critical (as defined for this standard), or no Critical Assets contain Critical Cyber Assets per this standard, the member of senior management must certify that fact. If the analysis determines that the responsible entity has Critical Assets and Critical Cyber Assets per this standard, the member of senior management must approve the list.	Annual review by a senior manager or delegate(s) has been added. R3 clarifies the requirements for a Responsible Entity with no Critical Assets or no Critical Cyber Assets.
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor Steven L Townsend

Entity Name Consumers Energy

	Comments	*Responses*
General	The standard needs to recognize the difference between securing a control center and securing a substation -- a substation does not have the same impact that a control center will have if it is compromised.	Only substations with Critical Assets require securing.
002-R1	Why is Blackstart (R1.1.6) part of the critical assets? During a Blackstart situation, cyber assets would not be used. If multiple options exist for Blackstart, does this remove the assets from the Critical Assets list? Does section R1.1.7 mean a substation that is capable of dropping 300 MW or a system that controls several substations that the total of the load dropped is greater than 300 MW?	If Cyber Assets are part of Critical Assets used for restoration, then they should be secured and protected to ensure that these assets function properly when they are required. These loadshed stations would be identified as Critical Assets, however, they may not have Critical Cyber Assets which require protection. (See FAQ 3 and FAQ 5.) No, in R1.1.7,each asset used for system restoration are considered separately. (See FAQ 7)
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3	If you only have dial-up access (R2.3), do the remaining standards apply?	
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Terry Doern
Entity Name	Bonneville Power Administration, Department of Energy

Comments	*Responses*
General	
002-R1	R1 has been modified.
R.1 Issue: The first sentence in the requirement states that the entity must identify their Critical Assets using their preferred risk-based assessment followed by R1.1, which provides a detailed list of all the Critical Assets that must be on the list. Requirement R1.1.9 then repeats the verbiage in the first sentence in R1. Recommendation: Delete the first sentence in R1 and move the verbiage from R1.1 to R1. Make the second sentence in R1, the second sentence in the new requirement.	
R1.1 -- A numbering issue: There is no need for a R1.1 if there is no R1.2. Recommendation: Make R1.1 part of R1 and renumber R1.1.1 thru R1.1.9 as R1.1 thru R1.9.	
002-R2	R2 has been modified.
R2.1: This should specify that the critical cyber asset is ONLY exclusively and/or remotely accessible via dial-up, direct physical connection or wireless, and does not use a routable protocol. It is unclear what situation is trying to be addressed. Please be specific.	
R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot. Incident response while required will be different. Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets	
R2.3 Issue: Requirement is confusing. It's not clear why a critical cyber asset would not need to be physically protected. Recommendation: Show an example similar to - 'What about an external laptop dial-up from home, connecting to a controlled location?'	
002-R3	Done.
R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot. Incident response while required will be different. Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets	

CIP-002 Drafting Team Responses to Comments

002-R4		
002-M1		
002-M2		
002-M3	M3 Issue: Measure refers to R3 twice in the same sentence when it should refer to R2 in the first reference. Recommendation: Change the first R3 to 'R2'.	The measures have been modified.
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3	1.3- Compliance: What is the definition of making the following documents available for inspection? Since these documents contain sensitive information - - is this an only on-site physical inspection? These documents shall not be mailed, e-mailed, faxed, or otherwise taken off-site! Recommendation - Change text to now read 'The Responsible Entity shall make the following available for inspection on-site, by the compliance monitor upon request'	The compliance section has been modified. Inspections of critical documents are normally done on-site. Proper procedures should be followed while handling Critical Infrastructure Information.
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Tim Hattaway
Entity Name	AECoop

	Comments	*Responses*
General	R1.1. and M2 Need more definition on risk-based assessment. What are the minimum elements this should include. I appreciate the flexibility of giving the responsible entity some flexibility here, but I'm also struggling with what this needs to be included in a risk assessment. R1.6-R1.7 Better define Regional Reliability Organization Does the 80% criteria mean the single largest generating unit within SERC? Those entities without large generators would not be affected by this requirement?	Suggesting an appropriate risk-based assessment methodology is outside the scope of the NERC Cyber Security Standards. RRO is defined in the NERC Functional Model. Correct.
002-R1	Further define routable protocol (i.e. IP address?)	R2.1 has been modified. Routable protocols has been clarified in the FAQs.
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Todd Thompson
Entity Name	Southwest Power Pool

	Comments	***Responses***
General	Suggest removal of R 1.2 -- R 1.10 to the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section.	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The measures have been revised to match the requirements.
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	Suggest this section refer to a “significant or material change” and should be 90 days.	The lists must be updated within ninety calendar days of the addition of, removal of, or modification.
002-M5	This section (in several areas) refers to “officers” whereas the other standards refer to “senior manager”. We recommend a standard term of “senior manager or designee”.	Senior manager is the term now used in all the cyber security standards. Option for delegate(s) has been added.
002-M6	This section (in several areas) refers to “officers” whereas the other standards refer to “senior manager”. We recommend a standard term of “senior manager or designee”.	Senior manager is the term now used in all the cyber security standards. Option for delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Tom Pruitt
Entity Name	Duke Power Company

	Comments	***Responses***
General	Overall -- Effective date of 10/1/05 for this standard is probably reasonable. Where "nuclear" ends and "transmission" begins is still an open issue. R4, M5, M6, D1.3.4 -- Says senior management officer in M5 & M6, says senior management in R4, senior management official in D.1.3.4.	Senior manager is the term now used in all the cyber security standards.
002-R1	R1.1.7: is senior management REALLY required? Who is that? A VP, a direct report to a VP? R1.1.7. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. R1.1.5: is the logic backwards here? Wouldn't a dial up asset need physical security MORE than electronic? R1.1.5. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter R1.2 -- Uses a different definition for Critical Assets than used in definitions Section. Need to clarify which is correct. Need to define "detrimental impact". R1.6 -- Does a common control system constitute "common system". If so, then essentially ALL generating resources of a large CA would fall under this requirement. An example of how purported flexibility is superseded by broad scope expectations	Option for delegate(s) has been added. R1 has been modified. The statement referring to dial-up access have been modified. Wording has been removed which referred to part of the definition of Critical Assets.
002-R2		
002-R3		
002-R4	B - R4 -- What level is considered senior management? Should say senior management or designee.	Option for delegate(s) has been added.
002-M1		
002-M2		
002-M3	M3 -- Correct the error ...Critical Cyber Assets identified under Requirement R3... should be R2.	Done.
002-M4	M4: 30 calendar days is too strict.	Changed to ninety days.
002-M5		
002-M6		
002-C1,1		

CIP-002 Drafting Team Responses to Comments

002-C1,2	1.2 -- How do we verify updates were made within 30 calendar days?	Annual review by a senior manager or delegate(s) has been added.
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	Tony Eddleman
Entity Name	Nebraska Public Power District

	Comments	*Responses*
General	This new standard imposes a significant overhead on smaller utilities and control areas that can not be justified by loss of those systems to the interconnected grid. The purpose statement indicates the critical assets should adversely impact the reliable operation of the critical bulk electric system assets. The standard should exempt any electric utility or control area with less than 1% connected load (estimated peak) or less than 1% of generation resources in the interconnection to which they are synchronized. As an example, the Eastern Interconnection is approximately 605,000 MW, so any "Responsible Entity" with less than approximately 6050 MW in the Eastern Interconnection would be exempt.	The purpose of CIP-002 has been modified. Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. Smaller utilities would have to comply only if they are identied underin the Applicability Section of CIP-002. They may have no Critical Assets under Required Critical Assets.
002-R1		
002-R2	Under section R2.1 - The Cyber Asset uses a routable protocol - describe intent of this section to more accurately depict the threat the standard is protecting against. Routable protocols can be secured, and non-routable protocols can be hacked, tapped, spoofed, etc.	See FAQ 2.
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4	Unders section C. Measures, M4 - Does the “or” mean that we can choose one method or the other, or that both methods must be followed? Under section C. Measures, M4 - What is meant by a “modification” of a critical cyber asset?	The measures have been modified. Modifications to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset. Additions to hardware, software or firmware could potentilly affect the operation of the Critical Cyber Asset.
002-M5		
002-M6	Under section C. Measures, M6 - does the senior management officer need to approve "modifications" (as used in M4) to critical cyber assets?	The lists must be updated within ninety calendar days of the addition of, removal of, or modification. Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Commentor	Tony Kroskey
Entity Name	Brazos Electric Power Cooperative

Comments		*Responses*
General		
002-R1		
002-R2		
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5	In Measure M5 the requirement for senior management officer's approval should be reworded to be approval of a member of senior management. The same for M6.	Annual review by a senior manager or delegate(s) has been added.
002-M6	In Measure M5 the requirement for senior management officer's approval should be reworded to be approval of a member of senior management. The same for M6.	Annual review by a senior manager or delegate(s) has been added.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Commentor	William J. Smith
Entity Name	Allegheny Power

	Comments	*Responses*
General		
002-R1	Requirements R1.1.1 through R1.1.9 are too prescriptive given the risk management approach to identifying critical cyber assets. They should be removed from the standard, and at most, be part of the FAQ as an answer to the question: What kinds of assets should I consider in my risk-based assessment?	Critical Assets have been split into "Required Critical Assets" and "Additional Critical Assets". The "Required Critical Assets" are supporting the critical operating functions and tasks of the interconnected Bulk Electric System. The requirement for a list of non critical cyber assets has been removed. See FAQ 8 for other criteria which a Responsible Entity might consider in their risk-based assessment.
002-R2	R2.3 - This section doesn't adequately take into account the substation environment. If someone accesses the physical perimeter of a substation, they would be able to cause an outage if sufficiently motivated regardless of the kinds of cyber precautions undertaken. The reason for physically protecting critical cyber assets located at substations is to reduce the risk to other critical cyber assets. Allegheny Power acknowledges that physical access to a critical cyber asset may also put other critical cyber assets within the same local electronic security perimeter at risk. Given the access controls placed on electronic security perimeters, however, physical access to a critical cyber asset in one local electronic security perimeter does not create a significant risk to critical cyber assets in other local electronic security perimeters. The standard should recognize that an adequate electronic security perimeter, in certain physical environments, is sufficient in regards to protecting critical cyber assets. CIP-002-1 R2.3 should be modified as follows: Critical Cyber Assets located at substations in which the local electronic security perimeter and its associated access points are completely contained within the substation control building require only an electronic security perimeter for the remote access without the associated physical security perimeter.	R2.1 has been modified for routable protocols within a substation or generating station where the routable protocol does not extend beyond the physical boundary of the facility.
002-R3		
002-R4		
002-M1		
002-M2		
002-M3		
002-M4		
002-M5		
002-M6		
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4