CIP-009 Drafting Team Responses to Comments

Commentor	Bob Wallace
Entity	Ontario Power Generation

	Comment	*Response*
General	OPG feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	Requirements, Measures and levels of non-compliance have been modified. Please see responses to comments by Richard Englebrecht, RGE. The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>>	
009-R2	Furthermore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	
009-R3	We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	
009-M1		
009-M2	We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.	
009-M3	Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from <<The Responsible Entity shall review and update recovery plan(s) annually.>> to <<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.	

CIP-009 Drafting Team Responses to Comments

009-C1,1

009-C1,2

009-C1,3 Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

009-C1,4

009-C2,1 Compliance 2.1 should be changed from <<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>> to <<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>

009-C2,2 As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004.

Compliance 2.2 should be changed from <<Recovery plan(s) have not been reviewed, exercised or training performed.>> to <<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>

009-C2,3 Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

Level 3 identifies a new requirement that should be identified in the requirements or measures section.

009-C2,4

CIP-009 Drafting Team Responses to Comments

Commentor	Carol L. Krysevig
Entity	Allegheny Energy Supply Company

	Comment	*Response*
General	Purpose - In this draft, NERC said that paragraph three was moved to the FAQ for the following reasons: it primarily explained the degree of recovery required in consideration of the expected impact and risk involved. However, it looks as though NERC actually moved the second and third paragraphs to the FAQs, and may have inadvertently removed the statement that describes the intent of this section. All that remains in the Purpose section of this draft is the boilerplate first paragraph (that's contained in all standards) that describes the overall purpose of Cyber Security. Following is the language provided in Draft 1: 1308 Recovery Plans (Draft 1 language) - The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function must establish recovery plans and put in place the physical and cyber assets necessary to put these recovery plans into effect once triggered. Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices. The above Draft 1 language indicates that the intent of the standard is as follows: to establish recovery plans and put in place the physcial and cyber assets necessary to put these recovery plans into effect once triggered. Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices. If the intent is NOT as stated above, then please provide alternative guidance.	Content was inadvertently left out during formatting and has been corrected.
009-R1	R1. - Allegheny Energy recommends that the EXERCISE of recovery plans for Power Stations should only be done for each representative type of equipment based on a plan derived by the responsible entity. Exact requirements should not be specified by this standard.	The requirement provides the suggested flexibility.
009-R2		
009-R3	R3 and M3 -- This Requirement and Measure appear to conflict. R3 says you have to update a plan within 90 calendar days of a major change, while M4 says plans need to be updated annually. The verbiage should be modified to state: to be updated at least annually, or within 90 days of a major change.	Requirements, measures, and levels of non-compliance have been modified and aligned.
009-R4	R4. -- This Requirement appears to be more of a measure that a requirement.	Requirements, measures, and levels of non-compliance have been modified and aligned.
009-R5		
009-M1		
009-M2		
009-M3	R3 and M3 -- This Requirement and Measure appear to conflict. R3 says you have to update a plan within 90 calendar days of a major change, while M4 says plans need to be updated annually. The verbiage should be modified to state: to be updated at least annually, or within 90 days of a major change.	Requirements, measures, and levels of non-compliance have been modified and aligned

CIP-009 Drafting Team Responses to Comments

CIP-009 Drafting Team Responses to Comments

Commentor	Dave McCoy
Entity	Great Plains Energy Cyber Security Task Force

Comment	*Response*
General	Please clarify the distinction between Requirement R1. "exercise its recovery plan(s) at least annually" and Measure M4. "conduct drills at least every three (3) years".	The Requirements and Measures have been modified. Reference to drills has been removed.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Don Miller / Ray Morella
Entity	FirstEnergy Corp

Comment		*Response*
General	The responsible entity should exercies their Recovery Plans when there are significant changes to the infrastructure or facilities.	Annual testing is a minimum; Responsible Entities can require additional testing.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Edwin C. Goff III
Entity	Progress Energy

Comment		*Response*
General		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	R5. This requirement references CIP-004-1; each standard should be self contained and not include references to other standards. Such cross-references embedded within other sections can lead to conflicts as individual standards may be at different versions or various approval stages.	The Standard has been modified. Reference to other reliability standards is allowable.
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

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

Comment		*Response*
General	National Grid believes CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents. Please see responses to comments by Richard Englebrecht, RGE.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>>	
009-R2	Furtherrmore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	
009-R3	We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	
009-M1		
009-M2	We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.	
009-M3	Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from<<The Responsible Entity shall review and update recovery plan(s) annually.>>to<<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.	
009-C1,1		
009-C1,2		

CIP-009 Drafting Team Responses to Comments

009-C1,3	Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.
009-C1,4	
009-C2,1	Compliance 2.1 should be changed from<<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>>to<<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>
009-C2,2	As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from<<Recovery plan(s) have not been reviewed, exercised or training performed.>>to<<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>
009-C2,3	Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Commentor	Gary Campbell
Entity	MAIN

Comment		*Response*
General	Masures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.	Requirements and Measures have been modified.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	The standard should not reference another standard. Either R5 should stand alone inthis standard or CIP-004-1	References are allowable.
009-M1	In M1, there was no mention of drills to be required for the recovery plans. If I was an sitting across from an auditor I would ask how you can measure me for something that you did not require of me.	Requirements and Measures have been modified.
009-M2	In M2, what is it specifically that is to be reviewed or updated?	Requirements and Measures have been modified.
009-M3	In M3, Is'nt the 90 day requirement in R3 important?	Requirements and Measures have been modified.
009-M4	In M4, this should be a requirement.	Requirements and Measures have been modified.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2	Level 2 - The recovery plan were only to be communicated? It seems were asking for more here.	Levels of Non-compliance have been modifed.
009-C2,3	Level 3 - It seems to me that if the types of events are important then the standard would specifiy these types otherwise you have set no minumum standard. Nor does the requirements tell me that I need to addres roles and responsibilites.	Levels of Non-compliance have been modifed.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Gerald Rheault
Entity	Manitoba Hydro

	Comment	*Response*
General	CIP-009-1 R1 indicates annual test frequency while M4 indicates drills every three years. The test frequency should be consistent. Is there a difference between "exercising its recovery plan" in R1 and "conduct drills" in M4? If not, then the terminology should be kept consistent between R1 and M4. Otherwise, the difference should be explained.	The Requirements and Measures have been modified.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor Guy Zito

Entity NPCC CP9

	Comment	*Response*
General	CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. It is unclear how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents. Please see responses to Richard Englebrecht, RGE.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>> Furthermore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	
009-R2		
009-R3	Requirement R3 appears to have the right intention, but its wording is too broad. Change from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	
009-M1		
009-M2	Measures M2 and M3 are duplicates. Delete Measure M2.	
009-M3	Measure M3 corresponds to Requirement R3. changeis required for Requirement R3. Measure M3 needs a similar modification from <<The Responsible Entity shall review and update recovery plan(s) annually.>> to <<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure should be deleted. This is covered in CIP-004.	
009-C1,1		
009-C1,2		

CIP-009 Drafting Team Responses to Comments

009-C1,3	Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.
009-C1,4	
009-C2,1	Compliance 2.1 should be changed from<<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>>to<<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>
009-C2,2	As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from<<Recovery plan(s) have not been reviewed, exercised or training performed.>> to <<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>
009-C2,3	Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Commentor	James W. Sample
Entity	California ISO

	Comment	*Response*
General	This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of "events that are necessary" could legitimately claim any of level 1, 2 or 3 noncompliance.	The compliance section has been modified to better align with the Requirements and Measures.
009-R1	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.	The drafting team believes annual testing, as a minimum, is appropriate.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	M1 and M2 should be merged.	Requirements and Measures have been modified to reflect the majority of comments.
009-M2	M2 and M3 are repetitive and should be merged.	Requirements and Measures have been modified to reflect the majority of comments.
009-M3	M3 contradicts R3.	Requirements and Measures have been modified to reflect the majority of comments.
009-M4	M4 is not consistent with R1 and needs to be clarified.	Requirements and Measures have been modified to reflect the majority of comments.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	Level 3 identifies a new requirement that should be identified in the requirements or measures section.	The compliance section has been modified to better align with the Requirements and Measures.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Jerry Heeren
Entity	MEAG Power

	Comment	*Response*
General	Requirements and Measures numbering scheme does not match.	Numbering has been changed.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Jerry Litteer
Entity	INL

Comment		*Response*
General		
009-R1	Exercise recovery plans at least annually should be coordinated with the test of the backup media (CIP-007 R11).	Testing requirement has been moved to this standard.
009-R2		
009-R3	R3 and R4. These two requirements seem to conflict. In any case, the backup recovery plans need to be kept current, tested, and 'as-built'. Waiting for seven days or 90 days may be fatal.	Requirements and Measures have been modified. The 90 day requirement has been retained.
009-R4	R3 and R4. These two requirements seem to conflict. In any case, the backup recovery plans need to be kept current, tested, and 'as-built'. Waiting for seven days or 90 days may be fatal.	Requirements and Measures have been modified. The 90 day requirement has been retained.
009-R5		
009-M1		
009-M2		
009-M3	M3. Annually may be to long. Documentation should exist that when a change in the 'system' is made that would affect the recovery plan, the plan is also updated.	Documentation must reflect that the plan was changed within 90 calndar days.
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Joe Weiss
Entity	KEMA

	Comment	*Response*
General	This section should reference ISA TR99.00.02-2004, Technical Report 2 -- Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment	The drafting team will review the ISA report.
009-R1	R1. The Responsible Entity shall create recovery plan(s) from cyber events for Critical Cyber Assets and exercise its recovery plan(s) at least annually. Recovery plans generally exist for Critical Assets for expected events but not necessarily for cyber events.	This requirement calls for entities to address recovery from a myriad of events.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	John Lim
Entity	Con Edison

Comment		*Response*
General		
009-R1	M5 requires drills at least every 3 years. R1 requires this at least annually.	Requirements and Measures have been modified
009-R2		
009-R3	Change R3 to: R3. The Responsible Entity shall review recovery plan(s) at least annually and update these recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.	Requirements and Measures have been modified
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Karl Tammer
Entity	ISO/RTO Council

Comment		*Response*
General	This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of "events that are necessary" could legitimately claim any of level 1, 2 or 3 noncompliance.	Compliance section has been modified
009-R1	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.	The drafting team believes annual testing, as a minimum, is appropriate.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2	M2 and M3 are repetitive and should be merged.	Measures have been modified
009-M3	M3 contradicts R3.	Measures have been modified
009-M4	M4 is not consistent with R1 and needs to be clarified.	Measures have been modified
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	Level 3 identifies a new requirement that should be identified in the requirements or measures section.	Compliance section has been modified and now match the requirements and measures sections.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Kathleen M. Goodman
Entity	ISO New England Inc.

Comment		*Response*
General	ISO-NE feels CIP-009 needs more work before it is ready for ballot. We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of <<events that are necessary>> could legitimately claim any of level 1, 2 or 3 noncompliance.	The Standard is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents. The compliance section has been modified.
009-R1	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.	The drafting team believes an annual exercise is appropriate. The Requirement was moved to R2 and explains that an exercise can range from a paper drill to a full operational and physical change over.
009-R2		
009-R3	We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>>to<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	Reference to major was removed.
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	Requirements and Measures have been modified.
009-M1	M1 and M2 should be merged.	Requirements and Measures have been modified.
009-M2	M2 and M3 are repetitive and should be merged.	Requirements and Measures have been modified.
009-M3	M3 contradicts R3.	
009-M4	Since (we recommend)Requirement R5 (be) deleted, the corresponding Measure should be deleted. This is covered in CIP-004.	Requirements and Measures have been modified.
009-C1,1		
009-C1,2	Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.	Levels of non-compliance have been modified.
009-C1,3		
009-C1,4		
009-C2,1		

009-C2,2

009-C2,3 Level 3 identifies a new requirement that should be identified in the requirements and measures section, Levels of non-compliance have been modified. or delete

009-C2,4

CIP-009 Drafting Team Responses to Comments

Commentor	Keith Fowler
Entity	LG&E Energy Corp.

	Comment	*Response*
General	We are in agreement with the comments submitted by the ECAR CIPP group.	See response to ECAR CIPP comments.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Ken Fell
Entity	New York Independent System Operator

Comment		*Response*
General	Rework Levels of Non-Compliance section to clearly categorize violations, rather than repeating violations across Levels.	Levesl of Non-compliance have been modified.
009-R1	Modify R1 from "The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise it’s plan’s per Risk Based Assessment process.	Requirements and Measures have been modified.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	Measure M1 and M2 are redundant.	Requirements and Measures have been modified.
009-M2	Merge M2 and M3.	Requirements and Measures have been modified.
009-M3		
009-M4	M4 is in conflict with R1.	Requirements and Measures have been modified.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	Level 3 Non-Compliance cites a new requirement "types of events that are necessary."	Levesl of Non-compliance have been modified.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Kurt Muehlbauer
Entity	Exelon Corporation

Comment		*Response*
General	R1 requires that recovery plans be exercised at least annually. M4 requires that the responsible entity conduct drills at least every three years. If a drill is different than an exercise, we recommend that the terms be defined. If a drill is not different than an exercise, we recommend that the testing periods for R1 and M4 be the same.	Reference to drills has been removed.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	s the training in R5 meant to be additional, focused training on recovery processes, or is it the general training referred to in CIP-004?	Training has been removed.
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	L.W. Brown
Entity	EEI Edison Electric Institute

	Comment	*Response*
General	Either the Purpose section or Requirement R1 should recognize that recovery plans may appropriately utilize various established business continuity and disaster recovery techniques, methodologies, and practices.	Added in the Purpose section.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel

Comment		*Response*
General		
009-R1		
009-R2		
009-R3		
009-R4	B.R.4--Recommend: If the changes are administrative in nature and do not affect the actions which need to be taken by individuals, the 7 day time frame is unduly short. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Assets within thirty (30) calendar days of development or modification.	The Standard has been modified to reflect these comments.
009-R5		
009-M1		
009-M2		
009-M3		
009-M4	C.M4--The Responsible Entity shall conduct drills annually and keep attendance records of its Recovery Plan (s) training.	The Standard has been modified to reflect these comments.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Larry Conrad
Entity	Cinergy

Comment		*Response*
General		
009-R1		
009-R2		
009-R3		
009-R4	R4."...updates or changes shall be communicated to personnel...with seven (7) calendar days..." Time period is un-necessarily short. Recommend that updates be communicated quarterly. Timing for updates and reviews needs to be standardized and more consistent throughout the documents generally using quarterly or annual reviews/updates.	Time period has been extended.
009-R5		
009-M1		
009-M2		
009-M3		
009-M4	M4--Requiring a drill "at least every 3 years" is too long a time period and the only place in the document where such a time period is recommended. Need standardization on the periodicity referenced throughout the documents, generally specifying annual requirements. Recommend change the drill requirement here to annual drill from at least 3 years.	The Requirements and Measures have been modified.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Laurent Webber
Entity	Western Area Power Administration

Comment		*Response*
General		
009-R1	R1: Must individual recovery plans exist and be exercised for every Critical Cyber Asset or is it adequate to have a single recovery plan for many similar assets? This is answered in the FAQ document.	It is sufficient to have one plan for similar assets.
009-R2		
009-R3		
009-R4	R4: This seems to be a conflicting requirement with CIP-003 R1-R3. CIP-003 requires the protection of Recovery Plans, while CIP-009 R4 requires the distribution of Recovery Plans. While it may be possible to meet both requirements, it will require careful coordination between the protection procedures and the distribution procedures. Such inter-related requirements should be identified with references to each other and careful consideration of the coordination effects.	The Requirements have been modified.
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Lawrence R Larson, PE
Entity	Midwest Reliability Organization

Comment	*Response*
General	Note that these should not be approved separately, (should not stand alone), so they are not ready until the others are.	A sentence has been added to the Purpose section joting that this standard is part of a group of standards.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Lee Matuszczak
Entity	U S Bureau of Reclamation

Comment		*Response*
General		
009-R1		
009-R2	R2 - Does NERC want to establish some baselines for contingency types to be addressed in test plans? Such events as site fires, extended loss of power, extended loss of access, loss of key staff, site destruction, armed takeover could be considered.	No, the risk assessment and the Recovery Plan should consider the types of event suggested, but is common practice to focus on degree of system/asset loss and not on senario based events.
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Linda Campbell
Entity	FRCC

	Comment	*Response*
General	The word -- major, should be clearly defined as it is subject to interpretation.	Reference to major was removed. Please see responses to comments by Pedro Modia, FPL.
009-R1		
009-R2		
009-R3	R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.	
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4	Does M4 speak to the attendance to the training or the drill? M4. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training	
009-C1,1		
009-C1,2	The words under Compliance section 1.2. really belong under 1.3. Data Retention. Compliance section 1.2. should be as follows: Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.	
009-C1,3	Compliance section 1.3. should be as follows: 1.3. Data Retention 1.3.1. The compliance monitor shall keep audit records for three (3) calendar years. 1.3.2. The Responsible Entity shall keep data for three (3) calendar years.	
009-C1,4		
009-C2,1		
009-C2,2		

009-C2,3

009-C2,4

CIP-009 Drafting Team Responses to Comments

Commentor	Patrick Miller
Entity	PacifiCorp

Comment		*Response*
General	Suggest an additional requirement in section C. Measures, that states: "The Responsible Entity will include recovery design considerations within the scope of projects that involve implementations, upgrades or modifications to Critical Cyber Assets" PacifiCorp distinguishes between Business Continuity Plans and Disaster Recovery Plans. This is a common approach across industries. These types of plans are not clearly distinguished within the standards in CIP-009-01. PacifiCorp Definitions: Business Continuity Plans are response procedures following events that impact a critical asset site and focuses on mobilization and relocation of employees to continue critical functions at an alternate location. Disaster Recovery Plans are the technical recovery procedures to recover a critical cyber asset at an alternate location.	
009-R1		
009-R2	For section B, R2 -- The language seems unclear. The language could imply that scenario-based plans are required. Scenario based planning is not considered a best-practice approach unless there is a high likelihood of a particular type of event. Following is a suggested amendment: "The Responsible Entity shall have recovery plans that allow for response to events of varying duration and severity"	Langugae has been modifed.
009-R3		
009-R4		
009-R5		
009-M1	M1 & M2 are duplicate entries and also seem repetitive to Section D, 1.2 Data Retention. Suggest that section C, M1.2 state: "The Responsible Entity shall maintain records of exercises or drills conducted and maintain those records in accordance to Data Retention Requirements. (3-Years).	Duplication removed.
009-M2		
009-M3		
009-M4	Section C, M4 combines two requirements and may be better suited to be separated or the attendance requirement clarified. The first requirement is that a drill is conducted at least every three (3) years. The second is that attendance records are to be kept on Recovery Plan training. Instead of training, is the intent to require attendance records of who participated in the drill? Requiring it for "training" may be too broad, implicating requirements to tracking attendees for awareness training, which can be in many forms.	Requirements and Measures have been modified.

CIP-009 Drafting Team Responses to Comments

009-C1,1		
009-C1,2	Section D, 1.2 Data Retention -- Seems to be duplicative of Section C, M1. If Section C requirements are clarified, this section would seem adequately stated.	Requirements and Measures have been modified.
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Paul McClay
Entity	Tampa Electric

Comment		*Response*
General	See FRCC comments	Please see responses to comments by Linda Campbell, FRCC.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Pedro Modia
Entity	Florida Power and Light

	Comment	*Response*
General	The word --major, should be clearly defined as it is subject to interpretation.	Reference to major was removed.
009-R1		
009-R2		
009-R3	R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.	The Standard has been modified .
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4	Does M4 speak to the attendance to the training or the drill?	M1 now addresses training attendance.
	M4. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training	Measures have been modified to reflect the Standard intent and comments.
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Pete Henderson
Entity	Independent Electricity System Operator

	Comment	*Response*
General	Though it may seem self-evident, the standard should not take as a given that all entities share the same understanding of what is required in a viable, "Recovery Plan". This standard should define the term, or at least provide guidance as to what is intended. This is particularly important as the "levels of non-compliance" portion of the standard suggests mandatory contents of the recovery plan (such as "types of events that are necessary") without ever defining these. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. An entity which neither updated its recovery plan in the past year, nor exercised it, nor included in it the types of "events that are necessary" could legitimately claim any of level 1, 2 or 3 non-compliance.	The complexity and level of detail will vary depending on several variable aspects to include the risk-based assessment. The Responsible Entity's risk assessment should identify events or circumstances that would initiate the Recovery Plan. Please see responses to comments by James Sample, California ISO
009-R1	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.	
009-R2		
009-R3	In R3, reword to state, "The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan".	
009-R4		
009-R5		
009-M1	M1 and M2 should be merged.	
009-M2	M2 and M3 are repetitive and should be merged.	
009-M3	M3 contradicts R3.	
009-M4	M4 is not consistent with R1 and needs to be clarified.	
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Randy Schimka
Entity	San Diego Gas and Electric Co

Comment		*Response*
General		
009-R1		
009-R2		
009-R3		
009-R4	R4 - The seven calendar day requirement in this section will be difficult to implement in a few instances, such as with substations that have Critical Cyber Assets. Typically, a large work force works in, on, and around these types of facilities. Communicating a high quality updated recovery plan to all personnel within 7 calendar days of modification could prove to be a daunting task. Our suggestion is something more reasonable such as 30 calendar days.	The Standard has been modified
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

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

	Comment	*Response*
General	CHGE feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents. Please see responses to comments by Richard Englebrecht, RGE.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>>	
009-R2	Furthermore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	
009-R3	We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	
009-M1		
009-M2	We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.	
009-M3	Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from <<The Responsible Entity shall review and update recovery plan(s) annually.>> to <<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure should be deleted. This is covered in CIP-004.	
009-C1,1		

CIP-009 Drafting Team Responses to Comments

009-C1,2

009-C1,3 Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

009-C1,4

009-C2,1 Compliance 2.1 should be changed from <<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>> to <<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>

009-C2,2 As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004.

Compliance 2.2 should be changed from <<Recovery plan(s) have not been reviewed, exercised or training performed.>> to <<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>

009-C2,3 Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

009-C2,4

CIP-009 Drafting Team Responses to Comments

Commentor	Richard Engelbrecht
Entity	Rochester Gas and Electric

	Comment	*Response*
General	NPCC feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. It is unclear how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>> Furthermore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	Requirements, measures, and compliance monitoring have been updated.
009-R2		
009-R3	Requirement R3 appears to have the right intention, but its wording is too broad. Change from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	Requirements, measures, and compliance monitoring have been updated.
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	Requirements, measures, and compliance monitoring have been updated.
009-M1		
009-M2	Measures M2 and M3 are duplicates. Delete Measure M2.	Requirements, measures, and compliance monitoring have been updated.
009-M3	Measure M3 corresponds to Requirement R3. change is required for Requirement R3. Measure M3 needs a similar modification from <<The Responsible Entity shall review and update recovery plan(s) annually.>> to <<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure should be deleted. This is covered in CIP-004.	Requirements, measures, and compliance monitoring have been updated.
009-C1,1		

CIP-009 Drafting Team Responses to Comments

009-C1,2		
009-C1,3	Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.	Requirements, measures, and compliance monitoring have been updated.
009-C1,4		
009-C2,1	Compliance 2.1 should be changed from<<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>>to<<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>	Requirements, measures, and compliance monitoring have been updated.
009-C2,2	As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from<<Recovery plan(s) have not been reviewed, exercised or training performed.>> to <<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>	Requirements, measures, and compliance monitoring have been updated.
009-C2,3	Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.	Requirements, measures, and compliance monitoring have been updated.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Richard Kafka
Entity	Pepco Holdings, Inc. - Affiliates

Comment	*Response*
General	Suggest that material found in the FAQ supporting this standard be relocated into the standard. Simmilar comment for other standards.	Some content was moved from the FAQ into the standard. The FAQ will be given consideration to become a NERC Reference Document.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Robert Strauss
Entity	New York State Electric & Gas Corporation

Comment		*Response*
General	NYSEG concurs with NPCC that CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. It is unclear how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.	The Standards is intended to address the recovery of Critical Cyber Assets from a myriad of events, not just cyber security incidents. Please see responses to Richard Englebrecht, RGE.
009-R1	Requirements R1 and R2 should be swapped. We recommend changing the first requirement from <<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>> to <<The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>> Furthermore, we recommend changing the second requirement from <<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>> to <<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>	
009-R2		
009-R3	Requirement R3 appears to have the right intention, but its wording is too broad. Change from <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>> to <<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>	
009-R4		
009-R5	Requirement R5 is covered in CIP-004. R5 should be deleted.	
009-M1		
009-M2	Measures M2 and M3 are duplicates. Delete Measure M2.	
009-M3	Measure M3 corresponds to Requirement R3. changeis required for Requirement R3. Measure M3 needs a similar modification from <<The Responsible Entity shall review and update recovery plan(s) annually.>> to <<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>	
009-M4	Since (we recommend) Requirement R5 is deleted, the corresponding Measure should be deleted. This is covered in CIP-004.	
009-C1,1		
009-C1,2		

CIP-009 Drafting Team Responses to Comments

009-C1,3	Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.
009-C1,4	
009-C2,1	Compliance 2.1 should be changed from<<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>>to<<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>
009-C2,2	As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from<<Recovery plan(s) have not been reviewed, exercised or training performed.>> to <<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>
009-C2,3	Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Commentor	Roger Champagne
Entity	Hydro-Québec TransÉnergie

	Comment	*Response*
General	CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	CIP-009 and CIP-002 have been modifed in response to the comments the drafting team received on Draft 2.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Scott R Mix
Entity	KEMA

Comment		*Response*
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 "Recovery Plans for Critical Cyber Assets".	Standard title has been changed.
009-R1	Requirement R1: add the following sentence: "The plan shall address recovery from physical disruption and damage, as well as cyber disruption and damage to the Critical Cyber Assets."	Requirements section has been modified in keeping with the majority of the comments. Included in this Standard is "...will follow established business continuity and disaster recovery techniques and practices." covers both physical and cyber disruption. Physical or Cyber loss of the Critical Cyber Assets is not split-out in this Standard.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Todd Thompson
Entity	Southwest Power Pool

	Comment	*Response*
General	This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of "events that are necessary" could legitimately claim any of level 1, 2 or 3 noncompliance.	Please see responses to comments by James Sample, California ISO.
009-R1	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.	
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	M1 and M2 should be merged.	
009-M2	M2 and M3 are repetitive and should be merged.	
009-M3	M3 contradicts R3.	
009-M4	M4 is not consistent with R1 and needs to be clarified.	
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	Level 3 identifies a new requirement that should be identified in the requirements or measures section.	
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Commentor	Tom Pruitt
Entity	Duke Power Company

Comment		*Response*
General	Overall -- Effective date of 10/1/05 for this standard is probably unrealistic due to the volume of systems that will require physically being at the system to be modified or enhanced to become compliant with this requirement.	The effective referes to the date the standard will be accepted into the compliance enforcement program. The implementation plan defines when compliance is expected.
	A - 4 -- typo? Any reference in this Standard to Critical. Why is this listed here and in A - 3 in the other standards?	The standard has been reviewed and typos removed.
009-R1	R1: create recovery plans and exercise the recovery plan at least annually - huge burden depending on the scope. If the scope is every piece of critical equipment, then this is darn near impossible.	If you have multiple Critical Cyber Assets such as substations, which have the same or similar Recovery Plans, exercising one plan for the common group will suffice.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		