CIP-008 Drafting Team Responses to Comments

Name	Bob Wallace
Entity	Ontario Power Generation

Comment	***Response***
General	Please see responses to comments on CIP-002.
OPG feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	
Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows << R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following: R2.1 System and application log file entries, R2.2 Appropriate physical access records, R2.3 Documented records of investigations and analysis performed, as available, R2.4 Records of any action taken including any recovery actions initiated. R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>	The Compliance and Measures section has been updated based on industry comments.
These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>	
008-R1	Reference to incident has been updated. The requirements section has been updated based on industry comments. Added the term adequacy to accuracy. This should be understood to cover not only that all information in the plan is accurate (e.g., correct phone numbers), but that it also meets the requirements of the entity.
Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from <<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>> to <<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>	The reason this was included is that the IAW SOP is required when reporting to the ES ISAC, the IAW SOP is what is defined by the ES ISAC. This requirement was also a requirement under the NERC 1200 standard. The items under Compliance were moved to a requirement, and measure updated.
Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.	
The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>	

CIP-008 Drafting Team Responses to Comments

008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2	We recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>	These sections have been updated based on comments and feedback from NERC staff responsible for NERC compliance
008-C1,3	We recommend changing Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>	These sections have been updated based on comments and feedback from NERC staff responsible for NERC compliance.
008-C1,4		
008-C2,1	We recommend changing Compliance 2.1.1 from <<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>	The compliance section has been updated based on industry comments
008-C2,2	We recommend changing Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>> We recommend changing Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to <<Cyber Security Incident Response Plan documentation exists but is incomplete>>	The compliance section has been updated based on industry comments.
008-C2,3	We request clarification on the threshold for Compliance 2.3.2.	The compliance section has been updated based on industry comments
008-C2,4	Change Compliance 2.4 from <<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist 2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>	The compliance section has been updated based on industry comments.

CIP-008 Drafting Team Responses to Comments

Name	Carol L. Krysevig
Entity	Allegheny Energy Supply Company

Comment		*Response*
General		
008-R1		
008-R2		
008-R3		
008-R4	R4. Does the Standard infer that the Regional Reliability Organization (or someone else) might be used as an INTERMEDIARY to report incidents?	Yes. While the entity may use an intermediary depending on regional structure, this does NOT however eliminate the entities responsibility to ensure that incidents are reported to the ES ISAC.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Don Miller / Ray Morella
Entity	FirstEnergy Corp

Comment	***Response***
General Why does the retention period need to be 3 years, 2 years should be acceptable.	Three years match the NERC compliance audit cycle.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Edwin C. Goff III
Entity	Progress Energy

Comment		*Response*
General		
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2	M2 - doesn't appear to match the section. It references requirements in another standard.	The measures section has been updated.
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

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

Comment	*Response*
General	Please see responses to Bob Wallace, Ontario Power Generation.

National Grid believes CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<<R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

008-R1

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows:
<<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>

CIP-008 Drafting Team Responses to Comments

008-R2

008-R3

008-R4

008-M1

008-M2

008-C1,1

008-C1,2 We recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>

008-C1,3 We recommend changing Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>

008-C1,4

008-C2,1 We recommend changing Compliance 2.1.1 from<<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>

008-C2,2 We recommend changing Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>

We recommend changing Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to <<Cyber Security Incident Response Plan documentation exists but is incomplete>>

008-C2,3 We request clarification on the threshold for Compliance 2.3.2.

008-C2,4 Change Compliance 2.4 from <<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

CIP-008 Drafting Team Responses to Comments

Name	Gary Campbell
Entity	MAIN

Comment		*Response*
General	Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement. Measures should not reference other standards. If the standard can not stand on its own then should the two be combined or is there something wrong? Some suggestion for Measures for this Standard: The Responsible entity has an incident response plan. The Responsible Entity has procedures on Classification of Incidents and Response Actions for Cyber Security Incidents. The Responsible Entity has reported all incidents to ESISAC. Levels of Compliance Specify review times in the requirements	The Requirements, Measures, and Levels of Non-compliance have been reviewed and modified.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4	Level 4 - This is a waste of a level. The way it is worded, if I have one document I can never be found to be level 4. This does not promote compliance. You would expect entities to have some level of completion to their documentation so maybe we should looking for at least half of the documentation completed to be level 4.	

CIP-008 Drafting Team Responses to Comments

Name	Guy Zito
Entity	NPCC CP9

Comment	*Response*
General	Please see responses to Bob Wallace, Ontario Power Generation.

CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<< R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

008-R1

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>

CIP-008 Drafting Team Responses to Comments

008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	NPCC Participating Members recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>
008-C1,3	Change Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>
008-C1,4	
008-C2,1	Change Compliance 2.1.1 from <<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>
008-C2,2	Change Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>> Change Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to << Cyber Security Incident Response Plan documentation exists but is incomplete>>
008-C2,3	Clarification is requested on the threshold for Compliance 2.3.2.
008-C2,4	Change Compliance 2.4 from<<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist 2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

CIP-008 Drafting Team Responses to Comments

Name	Hein Gerber
Entity	British Columbia Transmission Corporation

Comment	*Response*
General	Confirm if the title should be "Incident Response Planning" or "Incident Reporting and Response Planning". The former was used in the introduction title (A.1), the latter was used in the header and seems to be more accurate to the intent.	The title in the introduction section has been corrected.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	James W. Sample
Entity	California ISO

Comment	*Response*
General	The references to "incidents" should say cyber security incidents.	Reference has been changed.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Jerry Freese
Entity	American Electric Power

Comment		*Response*
General	The requirements in CIP-008-1 should be matched up with the measures. Also, CIP-001-1 may conflict with CIP-008-1.	The drafting team has corrected the alignment between requirements and measures. The drafting team will research potential conflicts with CIP-001-1
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Jerry Heeren
Entity	MEAG Power

Comment	***Response***
General Requirements and Measures numbering scheme does not match.	The drafting team has corrected the alignment between requirements and measures.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Jerry Litteer	
Entity	INL	
Comment		***Response***
General	If there is no requirement in the CIP standard for examining the logs, why is there are requirement to report incidents you do not know about.	CIP 008 Is intended to deal with the reporting of incidents. Monitoring of systems is covered in CIP-007 and Physical security monitoring is covered in CIP-006.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2	M2 those logs are only retained if an incident has been identified in the 90 day window for log retention.	The measure has been clarified.
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Jim Hiebert
Entity	California ISO

Comment	***Response***
General	This Section refers to the NERC Security Guidelines for the Electricity Sector Threat and Incident Reporting that uses the term 'any suspicious event' as a requirement for incident reporting. The concern is that 'any suspicious event' could include most firewall interceptions (and there may be hundreds/day) and that we have 60 minutes to report them [day or night] or be assessed a level-3 non-compliance penalty. We need better definition here.	Changes have been made to clarify this. The requirement is to report incidents. An event would not be reportable unless it is classified by the entity, using the entities classification procedures, as an incident. A FAQ has been added.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Joe Weiss
Entity	KEMA

	Comment	*Response*
General	FAQ 5. This should also reference ISA TR99.00.02-2004, Technical Report 2 -- Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment.	The drafting team appreciates the recommendation, and will review this reference document and add to the FAQ if applicable.
008-R1	R1. The Responsible Entity shall develop and document a Critical Assets incident Response Plan.	The requirement has been updated to refer to a Cyber Security Incident. "Cyber Security Incident" is defined in the standard.
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	John Lim
Entity	Con Edison

Comment	*Response*
General	The requirements and measures section is not consistent in qualifying incidents as cyber incidents. This standard only applies to cyber incidents.	References to "incident" were updated to refer to "cyber security incidents" where appropriate, as defined in the definitions section of CIP 008.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Karl Tammer
Entity	ISO/RTO Council

Comment	*Response*
General The references to "incidents" should say cyber security incidents.	References to "incident" were updated to refer to "cyber security incidents" where appropriate, as defined in the definitions section of CIP 008.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Kathleen M. Goodman
Entity	ISO New England Inc.

Comment	***Response***
General	Please see responses to Bob Wallace, Ontario Power Generation.
ISO-NE feels CIP-008 needs more work before it is ready for ballot. The references to <<incidents>> should say <<cyber security incidents>>.	References to incidents have been changed to cyber security incidents.
008-R1	
Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from <<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>> to <<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>> Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3. The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows<<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>	
008-R2	
We recommend creating a Requirement R2 as follows: <<R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following: R2.1 System and application log file entries, R2.2 Appropriate physical access records, R2.3 Documented records of investigations and analysis performed, as available, R2.4 Records of any action taken including any recovery actions initiated. R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>	
008-R3	
008-R4	
008-M1	

008-M2 The changes recommended for R2 call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

008-C1,1

008-C1,2 We recommend changing Compliance 1.2 from<<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>

008-C1,3 We recommend changing Compliance 1.3 from<<The Responsible Entity shall keep documents specified in this standard for three calendar years.>>to<<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>

008-C1,4 Compliance 1.4 stipulates a requirement that is not in the second posting.

008-C2,1 We recommend changing Compliance 2.1.1 from<<Documentation exists, but has not been updated with known changes with 90 calendar days.>>to<<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>

008-C2,2 We recommend changing Compliance 2.2.1 from<<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>>to<<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>

We recommend changing Compliance 2.2.2 from<<Incident response documentation exists but is incomplete>>to<<Cyber Security Incident Response Plan documentation exists but is incomplete>>

008-C2,3 We request clarification on the threshold for Compliance 2.3.2.

008-C2,4 Change Compliance 2.4 from<<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist

2.4.2 Cyber Security Incidents have occurred and none were reported to the

CIP-008 Drafting Team Responses to Comments

Name	Keith Fowler
Entity	LG&E Energy Corp.

Comment	***Response***
General	We are in agreement with the comments submitted by the ECAR CIPP group.	Please see responses to ECAR CIPP group.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York Independent System Operator	
Comment		***Response***
General	This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot. Retain use of "cyber security incidents" when referring to incidents within CIP.	Please see responses to CIP-002. References to "incident" were updated to refer to "cyber security incidents" where appropriate, as defined in the definitions section of CIP 008.
008-R1	Break R1.4-1.4.5 into a new R2, with corresponding measures.	The requirements have been clarified.
008-R2		
008-R3		
008-R4	Requirement R4 is too broad, and creeps into R3 territory. Modify to "The Responsible entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through a documented intermediary. Documentation to be submitted is outlined in R2.	Requirements have been modified.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon Corporation	
Comment		***Response***
General	The measures do not cover all aspects of R1 such as assessing, mitigating and containing. We recommend that the measures include all aspects of the requirements. If multiple responsible entities are affected by the same incident, do they all report it to the ES ISAC? We recommend that this scenario be clarified in a FAQ.	These sections have been updated. The expectation of the drafting team is that detail procedures for reporting to the ES ISAC will be included in the IAW SOP. However, the consensus of the drafting team was that each entity will have to report.
008-R1		
008-R2		
008-R3		
008-R4	We recommend removing the word ALL from R4. The IAW SOP has detailed criteria for what sort of incidents should be reported.	"all" has been removed
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel

Comment	***Response***
General Change the data retention from 3 years to 2 years throughout the document. This is one of the general comments, which pertain to all of the standards.	This is a required to support NERC audit at least once every three (3) years.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Larry Conrad
Entity	Cinergy

Comment		***Response***
General		
008-R1		
008-R2		
008-R3		
008-R4		
008-M1	The wording in the draft standard does not make sense and seem to be missing verbiage. It seems the intent is to require the documentation be reviewed annually and updated within 90 days of a known change. Wording needs to be fixed to clarify the meaning.	The wording has been clarified.
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Laurent Webber
Entity	Western Area Power Administration

Comment	***Response***
General	The definition of a Cyber Security Incident is extensive enough to include common events such as port scans or automated programs that attack databases and Web servers. Having to report such events within 60 minutes is an unreasonable requirement. The definition of a Cyber Security Incident must be more clear as to what must be reported or the requirement must allow each company to define Cyber Security Incident in the context of their systems. Suggest adding the phrase (is known or suspected to be of malicious origin) to the definition.	Changes have been made to clarify this. The requirement is to report incidents. An event would not be reportable unless it is classified by the entity, using the entities classification procedures, as an incident.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Lawrence R Larson, PE
Entity	Midwest Reliability Organization

Comment	*Response*
General	Note that, as NERC has already indicated, these should not be approved separately, (should not stand alone), so they are not ready until the others are.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Lee Matuszczak
Entity	U S Bureau of Reclamation

	Comment	***Response***
General		
008-R1	R1. - There is no discussion of testing or exercises throughout the standard. Perhaps this should be considered as a means of validating response plans.	The drafting team concurred with the comment; testing has been added to the standard.
008-R2		
008-R3		
008-R4	R4. - The last word in this requirement is "intermediary." It is unclear what an intermediary is, what their role is and if intermediaries must be identified and authorized to prevent false reporting.	While the entity may use an intermediary depending on regional structure, this does NOT however eliminate the entities responsibility to ensure that incidents are reported to the ES ISAC There is also a FAQ item related to the use of an intermediary.
008-M1	M1. - Physical incident response actions are discussed in this measure. It is unclear, however, how far this standard should attempt to go into the physical security and operational incident arena. This should probably be defined. What is a physical security incident? What is an operational incident? How do these incidents relate to cyber security incidents and who has authority and responsibility under incident conditions?	Incident classification has been left open for the entity to define within the standard.
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Linda Campbell
Entity	FRCC

Comment	***Response***
General	
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-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. 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.
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Lyman Shaffer
Entity	Pacific Gas and Electric Company

Comment	*Response*
General	Concern is that "any suspicious event" includes most firewall interceptions (and there may be hundreds/day) and that we have 60 minutes to report them [day or night] or be assessed a level-3 non-compliance penalty	Changes have been made to clarify this. The requirement is to report incidents. An event would not be reportable unless it is classified by the entity, using the entities classification procedures, as an incident. A FAQ has been added.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Patrick Miller
Entity	PacifiCorp

Comment	***Response***
General	
008-R1	
008-R2	For section B, R2, classification guidelines and examples should be offered.
	The FAQ includes references and url links that can be used to help guide entities. The drafting team will attempt to enhance the FAQ to provide additional guidance.
008-R3	
008-R4	For section B, R4 -- it is stated "...reported to the ES ISAC either directly or through an intermediary." Please define what qualifies as an intermediary (give examples).
	Please see the FAQ item related to the use of an intermediary. While the entity may use an intermediary depending on regional structure, this does NOT however eliminate the entities responsibility to ensure that incidents are reported to the ES ISAC
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Pete Henderson
Entity	Independent Electricity System Operator

	Comment	***Response***
General	The references to "incidents" should say cyber security incidents.	References to "incident" were updated to refer to "cyber security incidents" where appropriate, as defined in the definitions section of CIP 008.
008-R1	In R1, replace the word, "accuracy" by "adequacy".	Added the term adequacy to accuracy. This should be understood to cover not only that all information in the plan is accurate (e.g., correct phone numbers), but that it also meets the requirements of the entity.
008-R2		
008-R3		
008-R4		
008-M1	Measure M1 is worded poorly. The various documents may require periodic review, but surely that documentation does not need to define incident classification at least annually. As worded, M1 and M2 introduce new requirements that should be noted in the requirements section.	Measure has been reworded. Requirements and Measures have been reviewed and modified.
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4	In 1.4.1, it should only be required to retain log file entries relevant to the specific cyber security incidents, not all logs. In 1.4.2, it should only be required to retain records where relevant to specific incidents In 1.4., the reference to all cyber security incidents is redundant given the rest of Section D1.4.	1.4 has been moved to Requirement R2. The wording includes language specifying that only information specific to Cyber Security Incidents be retained.
008-C2,1	2.1.1 should read "Documentation necessary to show compliance with M1 exists, but has not been updated with known changes within 90 calendar days of known changes.	Levels of Non-compliance have been modified.
008-C2,2	In 2.2.1, it appears that the reference to "incident response documentation is actually a reference to the Cyber Security Incident Response Plan mentioned in R1. If so, the wording must be clarified, as otherwise the reference could be interpreted to be a reference to incident response records defined in Section C, item M2 and in Section D subsection 1.4	The wording has been updated to reference the plan.
008-C2,3		
008-C2,4	2.4 should be reworded as, " a documented Cyber Security Incident Response Plan does not exist."	The wording has been updated to reference the plan.

CIP-008 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co	
Comment		***Response***
General	Ready for ballot with minor changes - Introduction - Title should be: Cyber Security - Incident Reporting and Response Planning.	The title has been updated.
008-R1	R1 - 'periodic reviews' should be defined. An annual review would be preferred.	This has been defined in the standard as annual.
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

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

Comment	***Response***
General	Please see responses to comments from Bob Wallace, Ontario Power Generation.
CHGE feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows << R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following: R2.1 System and application log file entries, R2.2 Appropriate physical access records, R2.3 Documented records of investigations and analysis performed, as available, R2.4 Records of any action taken including any recovery actions initiated. R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>> These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>	
008-R1	
Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from <<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>> to <<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>> Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3. The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>	

CIP-008 Drafting Team Responses to Comments

008-R2

008-R3

008-R4

008-M1

008-M2

008-C1,1

008-C1,2 We recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>

008-C1,3 We recommend changing Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>

008-C1,4

008-C2,1 We recommend changing Compliance 2.1.1 from <<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>

008-C2,2 We recommend changing Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>

We recommend changing Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to <<Cyber Security Incident Response Plan documentation exists but is incomplete>>

008-C2,3 We request clarification on the threshold for Compliance 2.3.2.

008-C2,4 Change Compliance 2.4 from <<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

CIP-008 Drafting Team Responses to Comments

Name	Richard Engelbrecht
Entity	Rochester Gas and Electric

Comment	***Response***
General	Please see responses to Bob Wallace, Ontario Power Generation.
NPCC feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot. Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows << R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following: R2.1 System and application log file entries, R2.2 Appropriate physical access records, R2.3 Documented records of investigations and analysis performed, as available, R2.4 Records of any action taken including any recovery actions initiated. R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>> These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>	
008-R1	
Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from <<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>> to <<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>> Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3. The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>	

CIP-008 Drafting Team Responses to Comments

008-R2

008-R3

008-R4

008-M1

008-M2

008-C1,1

008-C1,2 NPCC Participating Members recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>

008-C1,3 Change Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>

008-C1,4

008-C2,1 Change Compliance 2.1.1 from <<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>

008-C2,2 Change Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>

Change Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to <<
Cyber Security Incident Response Plan documentation exists but is incomplete>>

008-C2,3 Clarification is requested on the threshold for Compliance 2.3.2.

008-C2,4 Change Compliance 2.4 from<<No documentation exists>> to
<<2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

CIP-008 Drafting Team Responses to Comments

Name	Robert Strauss
Entity	New York State Electric & Gas Corporation

Comment	***Response***
General	Please see responses to Bob Wallace, Ontario Power Generation.

NYSEG concurs with NPCC that CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<< R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

008-R1

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation

	submitted is outlined in Requirement R2.>>
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	NPCC Participating Members recommend changing Compliance 1.2 from <<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>> to <<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>
008-C1,3	Change Compliance 1.3 from <<The Responsible Entity shall keep documents specified in this standard for three calendar years.>> to <<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>
008-C1,4	
008-C2,1	Change Compliance 2.1.1 from <<Documentation exists, but has not been updated with known changes with 90 calendar days.>> to <<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>
008-C2,2	Change Compliance 2.2.1 from <<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>> to <<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>> Change Compliance 2.2.2 from <<Incident response documentation exists but is incomplete>> to << Cyber Security Incident Response Plan documentation exists but is incomplete>>
008-C2,3	Clarification is requested on the threshold for Compliance 2.3.2.
008-C2,4	Change Compliance 2.4 from<<No documentation exists>> to <<2.4.1 Cyber Security Incident Response Plan documentation does not exist 2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

CIP-008 Drafting Team Responses to Comments

Name	Roger Champagne
Entity	Hydro-Québec TransÉnergie

	Comment	***Response***
General	CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.	Please see responses to CIP-002.
008-R1	Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from <<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>> to <<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>	Reference to incident updated. Added the term adequacy to accuracy. This should be understood to cover not only that all information in the plan is accurate (e.g., correct phone numbers), but that it also meets the requirements of the entity.
	Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.	The requirements section has been updated based on industry comments.
	The new R1.3 (as we recommend) is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows <<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.	The reason this was included is that the IAW SOP is required when reporting to the ES ISAC, the IAW SOP is what is defined by the ES ISAC. This requirement was also a requirement under the NERC 1200 standard.
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		

008-C2,2

008-C2,3

008-C2,4

CIP-008 Drafting Team Responses to Comments

Name	Scott R Mix
Entity	KEMA

	Comment	***Response***
General	There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).	The drafting team has corrected the alignment between requirements and measures.
	In FAQ CIP-008-1.Q2, please add a clause indicating that the IAW program is voluntary from a U. S. Federal Government point of view based on the US Federal Government's ability to protect the information from disclosure under FOIA requirements, but required from a private industry point of view through this NERC standard.	That level of detail is in the IAW SOP, which is already referenced in the FAQ.
	FAQ-008-1.Qnew: Please describe the relationship between standard CIP-008-1 and standard CIP-001-1.	The drafting team researched potential conflicts with CIP-001-1 and added a FAQ.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2	Measure M.2 should move to standard CIP-007-1. There is no log retention requirement in standard CIP-008-1.	The wording has been removed.
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Todd Thompson
Entity	Southwest Power Pool

Comment	*Response*
General The references to "incidents" should say cyber security incidents.	References to "incident" were updated to refer to "cyber security incidents" where appropriate, as defined in the definitions section of CIP 008.
008-R1	
008-R2	
008-R3	
008-R4	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	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 must be modified or enhanced to become compliant with this requirement. R2 - R4 --Should these requirements be sub-bullets of R1?	A revised implementation plan has been developed. The Requirements section has been updated.
008-R1		
008-R2		
008-R3		
008-R4		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		