NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form C
CIP-008 through CIP-011

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8.	Annie Terracciano	Northern Lights Inc.	WECC 3										
9.	Aleka Scott	PNGC	WECC 4										
10.	Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12.	Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13.	Margaret Ryan	PNGC	WECC 8										
12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative		SERC	1, 3
4.	Northeast Missouri Electric Power Cooperative		SERC	1, 3
5.	N.W. Electric Power Cooperative, Inc.		SERC	1, 3
6.	Sho-Me Power Electric Cooperative		SERC	1, 3

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION C4 – CIP-008-5:

If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, most of the comments resulted in changes that improved clarity and did not require significant structural revisions. The consideration of comments according to major issues and standard sections follows.

References to EOP-004-2
The comments received for CIP-008-5 and EOP-004-2 both indicated support for handling the reporting of Cyber Security Incidents in CIP-008-5. EOP-004-2 received a much lower ballot approval in its most recent posting primarily for the one hour timeframe required for reporting Cyber Security Incidents. The commenters concern for EOP-004-2 was the lack of a timeframe for identifying a Cyber Security Incident. The required CIP-008-5 processes make clear that reporting to the ES-ISAC occurs within one hour of the analysis to determine whether an event would constitute a Cyber Security Incident. As a result, both drafting teams agreed to move the Cyber Security Incident reporting to the ES-ISAC to CIP-008-5. However, the SDT wishes to stress the reporting threshold is not necessarily one hour from the Cyber Security Incident occurrence. Instead, the threshold accounts for the analysis that must be performed in identifying the Cyber Security Incident. The incident could even have occurred much earlier without any observable behavior. Also, entities can still have a single reporting process to comply with the new versions of EOP-004 and CIP-008.

Applicability Section
Several commented that all instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". In response, we note that CIP-008-5 addresses incident response and reporting and the lack of external routable connectivity would not address this issue. It is possible for a Cyber Security Incident to occur on such cyber systems through insider attacks or other means of penetrating the physical or electronic boundaries. This does not create an inconsistency among the standards or implied requirement for monitoring because an entity can have a monitoring program to detect incidents that does not fully meet the requirements of CIP-006-5 and CIP-007-5.

There were several comments that stated CIP-008-5 should apply to Electronic Access Control and Monitoring Systems and Physical Access Control Systems. In response, applicability to these systems is unnecessary because the incident is associated to the BES Cyber Systems. Incidents occurring on perimeter systems would target the system and not the perimeter.

Other General Comments

One commenter requested clarification why the word "dated" has been added to the measures in these requirements. In response, dated documentation is used to clarify that such evidence is necessary to demonstrate time-based requirements.

There was a comment that suggested the word "annual" should be a defined in the NERC Glossary. In response, the SDT has chosen not to define annual because the periodicity for requirements in CIP may be different than requirements in other standards, and the definition of annual may have many interpretations.

Guidelines

One commenter suggested that references to DHS and NIST should not reside in the standard because NERC does not track those documents to ensure consistency. In response, the external references are dated to a specific version to address the case where future revisions do not remain consistent with the standard.

There was a comment that the definition of Reportable Cyber Security Incident is too vague and could result in the interpretation that activation of redundant systems causes the reporting not to be considered. In response, the SDT has clarified in the guideline that this is not the case. The SDT has added a clarification that the absence of lessons learned must still be documented.

One commenter proposed revisions requirements to "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach and has added to certain requirements "… identify, assess, and correct deficiencies…", which is explained in detail in the global summary portion of this document, above.

Background

One commenter stated that the background section for CIP-008-5 is contradictory in reference to measures by stating a numbered list is all-inclusive but measures serve only as examples. In response, the SDT notes that the background section states "A numbered list in the measure means the evidence example". This means the example evidence must include all of the items, but there may be other examples of evidence to meet the requirement. Both statements are true.

Requirement Part 1.1 and 1.2
Based on a comment, the SDT changed "Processes" to "One or more processes" for clarity.

Several commenters propose including additional specificity in the process for determining if an incident is reportable. The SDT has extensively discussed this issue, and the problem with additional specificity in Cyber Security Incidents is difficulty in exhaustively enumerating situations to report. Also, the reporting of incidents associated with damage alone can result in under-reporting, which does not meet the objective of this Requirement.

Requirement Part 1.4
Several commenters stated that 1.1 (responding) and 1.4 (handling) are essentially the same and proposed to delete 1.4**.** The SDT notes that while 1.1 addresses the initial identification and response to incidents, 1.4 addresses the actions to perform for resolving individual incidents. These are distinct activities.

One commenter suggested the that the applicability include low impact BES Cyber Systems because CIP-003-5 requires implementation of a policy addressing incident response, but CIP-003-5 intentionally centralizes all the requirements for low impact BES Cyber Systems which does not include specific elements of the plan.

There was a comment that suggested removing the parenthetical phrase for incident handling because recovery and post-incident analysis are covered elsewhere. In response, the SDT agrees that post-incident analysis is already handled in Requirement R3 of CIP-008-5 and clarifies the recover activities here pertain only to the incident. Recovery includes the confirmation that the incident has been resolved.

One commenter suggested adding wording to clarify physical security incidents need to be considered. In response, the SDT notes that the definition of Cyber Security Incidents includes physical intrusions.

Requirement Part 1.5

There was a comment that stated it is unclear if the list of internal and external contacts refer to those in EOP-004-2 or if there is a need to have a minimum list of contacts. In response, the internal or external contacts that an entity would need to include to ensure proper reporting for EOP-004-2 should be part of this list. Additional contacts are appropriate as necessary components of an incident response plan, but who resides in this list is left up to the entity.

A commenter suggested that the use of external organizations could result in double jeopardy with EOP-004-2. However, EOP-004-2 requires specific organizations whereas CIP-008-5 leaves the inclusion of additional external organizations up to the entity as a necessary part of the incident response plan. Double jeopardy does not exist here because there is not a requirement in CIP-008-5 to report.

One commenter proposed to replace the phrase "should receive communication" with "must be sent communication". In response, the SDT notes that this part of the incident response plan does not necessarily constitute required communication, but communication must be covered as a component of the plan.

Requirement R2

One commenter proposed adding an exception for the timeframes based on CIP Exceptional Circumstances. In response, the SDT notes that CIP Exceptional Circumstances have not applied to annual periodic performances requirements because of the flexibility in the timeframe of when an entity can perform this requirement.

Requirement Part 2.1

In response to a comment that 2.1 should expand to include all Cyber Security Incidents, the SDT continues to limit these requirements to Reportable Cyber Security Incidents because of the lessons learned and plan updates associated with each Reportable Cyber Security Incident. It is possible for Cyber Security Incidents to occur much more frequently.

In response to a comment, the SDT has removed the word "BES" before "BES Incident Response Plan" for consistency.

One commenter suggested revising the language of "at least once each calendar year, not to exceed 15 calendar months between executions" to "once each calendar year or a period not to exceed 15 calendar months between executions". The SDT notes that the language that exists is sufficient as currently written.

One commenter suggested using the term “exercise” instead of “test” because an actual exercise would suffice. In response, we had several comments to the contrary in the previous posting. The SDT uses test here because the word “exercise” is commonly used in reference to a planned execution.

One commenter suggested removing the lessons learned report from the measure because it is not part of the requirement. In response, we note that the measure only serves as an example, and a lessons-learned report would be an example measure for 2.1.

One commenter suggested that a full operational exercise should be required in the absence of an actual incident. In response, we suggest that the quality of an exercise does not depend on the type. It is possible to have a higher quality tabletop exercise than a full operational exercise.

One commenter suggested placing an “or” between all exercise examples, but this is not necessary because the “or” in the second bullet qualifies the entire list.

One commenter suggested expanding the scope of actual incidents that qualify as an exercise to include any Cyber Security Incident, but this would not exercise a key component of identifying and communicating a Reportable Cyber Security Incident.

One commenter proposed to remove any timeframes associated with the test. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

Two commenters suggested adding a specific reference to R1 to clarify the linkage, but the context of the Requirement in its use of Cyber Security Incident response plan is clear enough to avoid needing a direct linkage.

In response to several commenters, the word “plan(s)” was modified to “each plan” for added clarity.

In response to one commenter, the SDT qualified that the phrase “when responding to” is in regards to the Reportable BES Cyber Security Incident.

Based on comments, the SDT clarified exercises were for Reportable Cyber Security Incidents.

Based on comments, the SDT has removed the word “BES” from this requirement part.

Requirement Part 2.2

One commenter stated that this requirement part should be deleted because the main requirement part already addresses implementation and documented deviations are redundant with lessons learned. In response, the SDT points out that implementation of the plan does not necessarily mean that it be used during an incident or exercise. Some entities may interpret that a plan is implemented regardless of whether or not it is actually used. This additional requirement adds clarity in the expected outcome. The same is also true of lessons learned not having the full meaning of documenting deviations from the plan. However, we agree that the documentation should not necessarily occur concurrent with the incident and have modified this requirement part accordingly.

One commenter suggested requiring documentation for the lack of deviations from the plan. In response, we do not agree this language is necessary. The absence of deviations may be a common occurrence and the requirement to have such documentation is highly administrative. We believe this is different than the case of not having any lessons learned which should be a much less common occurrence.

One commenter suggested requiring plan updates for new vulnerabilities and threats. The SDT agrees this would be appropriate if the plan were not sufficient to address new vulnerabilities and threats, but measurable criteria for what constitutes a new vulnerability or threat does not exist and could likely not be determined by anyone other than the Responsible Entity.

In response to a comment, the SDT replaced the phrase “incident response plan” with “Cyber Security Incident response plan” for consistency.

In response to several commenters, the word “plan” was changed to “plan(s)” for consistency.

Requirement Part 2.3

One commenter proposed that 2.3 should be moved to the compliance evidence section of the standard. In response, the evidence retention section cannot add a new requirement, and without 2.3 there is no requirement to retain evidence of the incident.

Several commenters suggested the language for requirement part 2.3 include a retention period, but this requirement was modified in response to comments that the retention period be covered in the compliance evidence section of the standard. As a result, part 2.3 includes the requirement to retain the records, which may not have been necessary to retain anywhere else in the standard, and the compliance evidence section defines the retention period.

There were several commenters who stated that this requirement part could have double jeopardy with EOP-004-2, but lack of documentation for reporting purposes would not be a violation of CIP-008-5. Also, EOP-004-2 evidence retention does not necessarily cover evidence related to a Cyber Security Incident.

One commenter suggested storing the evidence in encrypted form. In response, CIP-011-1 addresses the storage of BES Cyber System Information. Specific implementation of this requirement is appropriately left to the entity.

The SDT has removed the word "relevant" responding to comments that it adds unneeded subjectivity.

One commenter questioned whether three calendar years is sufficient for retaining incident evidence for law enforcement, state, and federal requirements, but the evidence retention is a minimum for the purpose of the Standard. If additional requirements outside of the NERC Reliability Standards indicate a longer retention period for a particular entity, then the entity would choose the longer period. There is no conflict.

Requirement R3

One commenter proposed that the main requirement should more closely align with CIP-009-5 R3 and focus on maintaining, and not implementing, the plan. The SDT agrees.

One commenter suggested the word "full" be deleted from "full operational exercise" because it is unclear what it implies. The SDT agrees.

Requirement Part 3.1

Several entities have commented this requirement part is duplicative with testing in R2 and monitoring for plan changes in R3. The SDT agrees and has deleted this requirement part.

In response to a comment that proposed to consider additional changes that trigger a review of the incident response plan, the lessons learned requirements suffice for updating the plan in response to incidents. Changes to the security

configuration already trigger updates in requirement part 3.4. In many cases the incident response plan is written at a high enough level to preclude necessitating changes in response to new threats and vulnerabilities.

Requirement Part 3.2

There were several comments that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.2, 3.3 and 3.5 into a single requirement part 3.1. The additional requirement part 3.4 for monitoring plan changes and 3.5 has collapsed into a single requirement part 3.2. Some commenters suggested that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

One commenter suggested tying this requirement explicitly with both 2.1 and 2.2. In response, the cross-referencing of requirements could cause more confusion than clarity. The SDT feels this explicit tie is best accomplished in the guidance.

One comment proposed to remove any timeframes associated with plan updates. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

There was a comment that suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

One commenter suggested changing this requirement part to include language for consistency with the ERO Event Analysis Process. The ERO Events Analysis Process is not a NERC Reliability Standard, and the SDT is not mandating referenced actions that are not developed through the NERC process or an equivalent ANSI Certified process. The SDT also notes that the proposed requirement language leaves flexible “how” to perform the requirement. Entities may choose to follow the procedures outlined in the ERO Events Analysis Process to comply with the requirement, but are not required to. The SDT also understands that the NERC CIPC is planning to form a working group to develop guidelines for analyzing cybersecurity events using a parallel process to the recently approved ERO Events Analysis Process. Specifying

that the ERO Events Analysis Process be used in response to CIP-008 Reportable Cybersecurity Incidents is premature and will remove any perceived or required flexibility in developing cybersecurity-specific procedures under that group.

Several commenters suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

In response to one comment, the SDT has added examples of evidence for lessons learned.

In responses to multiple comments, the SDT changed the phrase “within 90 days” to “not to exceed 90 calendar days” for clarity.

Requirement Part 3.3
In response to a comment, it is not necessary to modify this requirement to state “update as needed” because the requirement part ties to “any lessons learned” which carries the same effect.

Requirement Part 3.4
One commenter suggested reverting to previously approved language for updates and notes that evidence to meet this requirement would include lists of technology changes. In response, the SDT notes that such evidence would be required in the previously approved version if specific technology was referenced in the plan. The changes identified here are to provide additional clarity in the types of changes that should trigger an update.

Several commenters proposed that the term “technology changes” needs to be defined. The SDT notes this only includes technology changes that would impact the ability to execute the plan. Because this term is so contextual to the plan, it would cause more problems to define it. Entities should review their plans to see whether or not they have technology as a key element of the plan. The guidance specifies that “technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.”

Requirement Part 3.5
Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the evidence examples of distributing the plan could result in a violation of confidentiality, but, while each example can specify additional mechanisms to preserve confidentiality, this was not the intention of the measure. In some cases, incident response plans may not contain confidential information.

VSLs

One commenter recommended that the documentation of the absence of any lessons learned should be included in the VSLs. In response, the absence of lessons learned has been included in the VSL.

One commenter recommended that the VSL should not include failure to follow the plan during an incident and the VSL associated with lack of documentation of deviations suffices. The SDT agrees and does not need to modify the VSLs.

QUESTION C8 – CIP-009-5:

If you disagree with the changes made in CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-009-5 expressed in comments were (1) backup media verification procedures in requirement parts 1.4 and 2.2, (2) data preservation procedures in 1.5 and (3) timeframe requirements in Requirement R3 on the lessons learned and plan update activities. The consideration of comments according to major issues and standard sections follows.

Applicability

One commenter suggested that the applicability for all requirements in this standard should limit to Medium Impact BES Cyber Systems at Control Centers to appropriately focus on the higher risk cyber systems and avoid conflict with PRC Standards. In response, the loss of Medium Impact BES Cyber Systems has impact to the BES and the recovery operation for these cyber systems should be addressed in this standard.

The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs, which means testing for substations and generating plants that are not high impact is not included. A commenter asked for confirmation on whether this was the SDT's intent. Yes, it was.

One comment suggested that applicability to associated Cyber Assets should be removed because the FERC has not directed to do so. In response, these continue to apply from all prior versions to the associated Cyber Assets.

Other General Comments

One commenter proposed modifying the main requirement part and corresponding VSLs for R2 and R3 to allow for a flaw remediation process. In response, we have modified the main requirement part for R2 to eliminate the zero tolerance obligations because of the possible magnitude of plans and backup media which require testing. However, we do not incorporate the same changes for R3 because the requirements here do not have the same zero-tolerance concerns and they specify the procedures that must be in place to ensure better response plan flaw remediation.

Guidelines

Several commented that application guidelines should be included for CIP-009-5, and we have added these.

Background
One commenter suggested that the background section is contradictory by saying that measures are not all-inclusive but numbered list provide an all-inclusive example. In response, the background section states, "A numbered list in the measure means the evidence example includes all of the items in the list." This refers to the single example and is different than an all-inclusive list of evidence examples. Accordingly, if an entity did not provide all parts of the numbered list of evidence, then they would not fully meet the requirement. However, they could still provide alternate forms of evidence outside of the example.

Measures
There was a comment that the measures should be clarified with the following language: "Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." The SDT notes that the language in the requirement is clear and that the measures provide adequate examples of evidence. Each requirement part addresses different levels of that may be expected.

Requirement R1
One comment proposed to add a requirement for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. They also commented that the requirement should state the level of granularity required for a plan. In response, it would be problematic to standardize and audit a normal operating role. The SDT is uncertain as to the meaning of this term. The purpose of this standard is "to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES." It is inappropriate to specify the level of detail required for a recovery plan.

Several commenters suggested that the standard is not clear whether the recovery plans are for recovery of the asset, system, or function. In response, the stated purpose for the standard is "to recover reliability functions performed by

BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES."

One commenter asked the following: "is a Business Continuity Plan, where operations are transferred from the main control center and continued at a back-up control centre, considered a recovery plan?" In response, this could constitute a recovery plan according to Requirement R1 with the additional components listed in the requirement parts. However, restoration of the reliability function meets the purpose of this standard.

Requirement Part 1.1
One commenter suggested removing "specific" activations from the measure, and we have done so.

One commenter suggested the minimum conditions for activating a response should be specified. Otherwise entities can choose an inappropriately high bar. In response, any minimum enumeration of recovery conditions would equate to defining system failure and doing so for a highly variant population of systems across the BES is not feasible.

Requirement Part 1.3
Several commenters suggested changing the phrase "BES Cyber System" to "applicable Cyber Assets". However, "restoring BES Cyber System" functionality describes the objective of the requirement part and not the applicability.

One commenter suggested addressing FERC Order 706 paragraph 748 by appending the suggested text from the Order to this Requirement Part addressing backup media. We agree this is clearer and have incorporated their suggestion in requirement part 1.4 because of the difference in applicability from 1.3.

One commenter suggested modifying this requirement part measure to provide alternate forms of evidence and avoid the interpretation that evidence must be shown for each occurrence in a high-frequency operational requirement. In response, the SDT has modified the measure according to these suggestions.

Several commenters suggested removing the qualifier word "successfully" from the measure and the SDT has done so.

One commenter suggested including documented configuration settings, documented build/restoration procedures, and retention of installation media for example evidence. The SDT has added these to the technical guidelines section of the standard.

Several commenters suggested replacing the word “recover” with “restore” to describe the purpose of the backup media. In response, we retain the use of “recover” to avoid confusion. Both words mean to return something to a normal or former condition, and the SDT finds these words can be used interchangeably while still communicating the same concept.

One commenter noted the measure is missing an “and”, and the SDT has corrected this oversight.

Requirement Part 1.4

Several commenters expressed confusion around the term “initially” in the requirement, and the SDT has removed this term by tying the verification processes to the backup and storage processes in 1.3. The resulting language should provide more clarity and eliminates the term “initially”.

One commenter suggested addressing FERC Order 706 paragraphs 732-734 in this requirement section or moving this to guidance. In response, the resulting directive in paragraph 739 is addressed by the proposed text to address 748. Another commenter also supported the proposed language in the FERC Order. In response, verifying the operability of backup media is addressed by verifying successful completion and addressing failures of the backup process. Short of performing a full restoration, monitoring the backup process provides the appropriate assurance in the integrity of the backup for constantly changing systems. We have also added further guidance for this requirement part.

One commenter stated that FERC did not express concern over Physical Access Control Systems and Electronic Access Control and Monitoring Systems and applicability for these should be removed. In response, we retain the applicability from previous versions of the standard to which the FERC Order was addressed.

Several commenters requested further clarification about the meaning of verification of backup media. In response, the verification of backup media is dependent upon the tool performing the backup. This could include checking for read/write errors or performing a checksum during the backup operation. The SDT has clarified this requirement to read verification of successful completion.

One commenter suggested this requirement part be modified to address 3rd parties performing the backup or providing a backup, and the requirement has been modified to address these concerns.

Several commented on the 90 day retention period for the logs specified in this requirement part measure. In response, the reason for having 90 day retention for BES Cyber System logs is the potentially large volume, but there is no such concern for the evidence example for this requirement part.

One commenter does not believe this requirement part belongs as written here, and we note the overall modifications to this requirement part better fits the overall objective of Requirement R1.

One commenter stated that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to regularly verify the redundancy and address failures.

One commenter asked the following questions: If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? In response to these questions, the currently proposed requirement does not specify a timing that is sufficient for verification due to the widely varying backup methodologies that exist for the applicable systems. A printed log or periodic automated sampling of the backup process would be considered sufficient evidence for this requirement.

One commenter stated that the only way to verify backup completion is to restore from backup. In response, completion of the backup process or routine is different than successful restoration, and we contend the former can be verified outside of a full restoration.

Requirement Part 1.5

Several commenters suggested replacing the word "event" with the phrase "Cyber Security Incident" to better scope when it is necessary to preserve data. In response, we have made this change and modified the requirement to better qualify the purpose of preservation. The requirement should read clearly that data must be retained until a Cyber Security Incident may be ruled out as the cause of the recovery operation.

One commenter suggested removing this requirement part because it addresses forensics and not recovery. In response, this requirement part ensures data collection procedures are included in the recovery plan to allow the performance of after-the-fact analysis. This is appropriate to require as part of the recovery operation.

One commenter suggested that with changes to the definition of CIP Exceptional Circumstances to include "an imminent or existing hardware, software, or equipment failure", this requirement would never invoke. Their proposed language incorporates the concept of CIP Exceptional Circumstances, and we have included much of the proposed wording in the revised requirement part. The commenter also proposed to limit this requirement part to Medium Impact BES Cyber Systems at Control Centers, but neither the threat nor the operational circumstances for field assets preclude applicability for this requirement part. This requirement allows sufficient flexibility to apply in widely varying environments. The modifications here also address other comments about clarifying the procedures should not impact reliability.

One comment suggested that the PRC Standards already cover this for relay misoperation, but these standards do not address specifically the failure of a Cyber Asset nor do they address the preservation of data from Cyber Assets.

One commenter stated that this requirement implies an obligation to mirror data in the measure, should be left up to the entity to determine whether or not to delay recover for the purpose of preserving data, and an entity cannot determine the preservation of data given the many ways in which a system can fail. In response, we first note that a measure is only an example and does not imply an obligation to mirror data. Second, the SDT has taken an exception to add an explanatory note in the requirement cautioning against impeding recovery for data preservation. Finally, this requirement part does not envision an entity determining every way in which a Cyber System can fail. This only obligates the entity to include data preservation procedures in the recovery plan. There was a second comment on the guidance language in the measure, and the SDT agrees the language does not readily associate itself to the requirement and has been removed.

One comment suggested that this requirement part should be part of root-cause analysis and not impede system restoration. The SDT agrees and notes the requirement part does not address forensics but only the preservation of data to support root-cause analysis and forensics after-the-fact.

Requirement Part 2.1

One commenter suggested for this requirement part and requirement part 2.3 that the word “exercise” should be used in place of “test” since an actual recovery operation can be used for compliance. However, several commenters suggested the converse in the last posting, and we are not compelled the difference in terminology changes the meaning of the requirement.

One commenter suggested revising the language of “at least once each calendar year, not to exceed 15 calendar months between executions” to “once each calendar year or a period not to exceed 15 calendar months between executions”. The SDT notes that the language that exists is sufficient as currently written.

Several commenters requested clarity about whether or not each recovery plan must be tested annually. In response, we have modified this requirement to explicitly state that each recovery plan must be tested as was the intent. We do not specify a representative sampling of plans be tested as some suggest because the proposals do not include enough information to objectively determine what constitutes a representative sample. However, we do note that it is possible to singularly test multiple cyber systems if they are similar in nature.

One commenter suggested that all backup media should not be required for testing but only the one needed for recovery, and we have modified the requirement to include this condition.

One commenter suggested that “or” should be added to the first bullet point or it is otherwise required. In response, the or in the second bullet point modifies the entire list.

Requirement Part 2.2

One commenter asked if this requirement part includes a media test and whether this can be performed on a sample system. In response, this can include a media test on a sample system provided some verification to ensure the information is current and useable occurs. We have modified the measure for this requirement part to make this clearer.

One commenter suggested allowing an actual recovery operation to substitute for the testing of backup media, and we have made this change.

One commenter proposed to replace the requirement with “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar

year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." The concern surrounds possible double jeopardy with EOP-008 and clarity around "compatibility with current system configurations." In response for EOP-008-1 R7, failure to meet this requirement does not indicate a failure for EOP-008-1 and vise-versa. This requirement concerns the testing of backup media, which may not be used for recovery with EOP-008-1. For the proposed language, we have incorporated the "representative sample of information" in testing to clarify the obligation, but we retain the purpose of verifying compatibility with current system configurations. Only ensuring the usability of backup media does not capture the intent that the backup media is currently usable for performing the BES Cyber System function.

One commenter suggested striking the phrase "to ensure that the information is useable and is compatible with current system configurations" and believes it should be left up to the Responsible Entity to determine, whether another commenter requested further clarification about this phrase. In response, the testing of backup media alone is not specific enough to ensure clarity of the requirement. The phrase in question is necessary for entities to know what they should be testing. We have added additional technical guidelines for this requirement.

One commenter suggested that this requirement should state that a tabletop exercise should not be permitted. In response, the testing of backup media may be performed as a separate process or as a part of the recovery plan exercise. There is not a need to specify which type of exercises aligns with this process.

One commenter suggested that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to test the redundant systems in accordance with this requirement part.

Several commenters proposed the phrase "validate the integrity of the stored information" as a substitute for current language regarding the testing of backup media. In response, validating the integrity of the information can be interpreted widely from a bit comparison to a sampling. We believe our proposed revisions provide enough specificity and flexibility to be widely applied.

One comment proposed to focus the requirement on backup media rather than information used for recovery. In response, we use the term information here because of the various ways entities implement backup policies, which may include replication technologies. Backup media was not well understood by the team and many participants to include replication.

Requirement Part 2.3

Several comment that the measure references performance of this requirement prior to the Effective Date, and that this requirement part should be included in the Implementation Plan. In response, we have removed this language from the measure and added this requirement part to the Implementation Plan.

One commenter suggested testing a representative of a plan with a rationale that High Impact BES Cyber Systems already have a requirement to test backup media annually. In response, we do not see a significant change in the proposed wording. The requirement to test backup media does not require a full operational restoration.

One commenter requested clarity that all recovery plans do not have to be tested at the same time. In response, the requirement only specifies the obligation to test recovery plans at a periodicity. It would not violate the requirement to test individual plans at different periods while still meeting the periodicity obligation.

One commenter requested a basis for the 36 months period. In response, we incorporated this timeframe from the FERC Order 706 directive.

One commenter suggested testing a “representative” rather than “each” BES Cyber System. In response, if an entity can test a representative BES Cyber System for multiple systems, then they have complied with the requirement to test “each” BES Cyber System.

One commenter noted that an entity may have several failure scenarios and it is unclear if all of these must be tested. In response, we have added guidance in the technical guidelines section of the Standard to clarify that not all failures scenarios must be tested, but that the test should ensure the plan is up to date and test at least one process to restore the applicable cyber systems.

One commenter suggested that EOP-008 R6 should suffice for this requirement part. In response, EOP-008-1 R6 requires independent backup functionality, but this does not imply an obligation to perform a functional test. The compliance processes to comply with EOP-008-1 should certainly ease compliance with this requirement part.

Several respondents asked whether a full operational exercise means a bare-metal recovery and comments that doing so would be cost prohibitive, while another commenter suggested also requested further clarification around

the term “operational exercise”. In response, the SDT has provided well established definitions of operational exercises that would comply with the requirement, which do not imply a full recovery demonstration.

Requirement R3

Requirement R3 has been modified to correspond with similar commenter suggestions in CIP-008-5 R3.

One commenter suggested that Requirement R3 does not include defined roles and responsibilities. As we understand the comment, the roles and responsibilities refer to those required parts of the response plan specified in Requirement R1.

Requirement Part 3.1

Several commenters noted that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.1, 3.2 and 3.4 into a single requirement part 3.1. The additional requirement part 3.3 for monitoring plan changes and 3.4 has collapsed into a single requirement part 3.2. Some comment that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

A few commenters suggested updating plans based on lessons learned is not necessary because these changes would be captured in technology and personnel changes. In response, the updates here capture improvements to the plan as determined through a lessons learned exercise.

One commenter suggested that the evidence collected in requirement part 1.5 should be part of the review process. They also commented that other related plans (i.e. configuration management plans) be updated as necessary as part of the review process. In response, the evidence collected in requirement part 1.5 may not be reviewed by a third party and we do not feel it is necessary to specifically call out this activity in the requirement part. Also, we cannot add an obligation to update other plans as necessary in a way that would be objectively measurable.

One commenter suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

Several commenters have suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

Several commenters stated that requiring entities to perform lessons learned is counterproductive because it encourages entities not to admit there is a deficiency in the first place. In response, the inclusion of a lessons learned process provides a standard practice across the industry, which would otherwise be inconsistency applied at best. Furthermore, it addresses a FERC Order 706 directive to include lessons learned processes as part of a recovery plan test.

Requirement Part 3.3

One commenter suggested modifying the references to other standard requirement parts, removing references to individuals and modifying the communication of plan updates to be more specific. In response, the SDT has made several modifications to Requirement R3 to align with modifications to CIP-008-5 that address these concerns.

Several commenters proposed removing this requirement and addressing plan updates in guidance, but placing the plan items that would trigger a change in guidance would add a high degree of subjectivity to the requirement. Specifying what changes should constitute an update ensures objectivity in demonstrating compliance with this requirement.

One commenter proposed removing this requirement or clarifying the tie back to Requirement R1.2. In response, this requirement is necessary to ensure the recovery plan remains current and carries forward from the requirement to update on any changes. They also expressed concern that this requirement part could be interpreted that a change to any plan must be communicated to all individuals specified in requirement part 1.2. In response, we have removed the explicit tie to requirement part 1.2 to avoid such an interpretation.

One commenter suggested that the plan maintenance would create an undue compliance burden. In response, the SDT notes this requirement carries forward from previous versions and ensures the recovery plans remain up to date through organizational changes.

Requirement Part 3.4

Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the distribution of plan updates should include some irrefutable evidence on the part of the receiver. In response, we do not believe the added qualification would have the desired benefit. Individuals can choose to ignore the content regardless of the evidence of receipt.

One commenter stated that the example evidence for communicating plan updates is a poor choice because of the confidentiality of such information. In response, the examples do not necessitate the sharing of sensitive information but only that the individuals be notified. We have included additional guidelines to consider the sensitivity of the information when sending the required notifications.

VRF

One commenter proposed that the VRF should be Lower for consistency with other requirements. In response, we retain the previously FERC approved VRF of Medium for this requirement because failure to have restoration procedures directly affects the BES reliability function of High and Medium impact BES Cyber Systems.

VSLs

The VSLs have been updated corresponding to changes made to requirements in CIP-009-5.

One commenter suggested that “within 30 days” should be changed to “greater than 30 days”. The SDT agrees and has made this change.

Several commenters suggested that the moderate VSL for Requirement R1 should address “one” and not “all” missing elements of the plan. The SDT agrees and has made this change.

One commenter suggested that the VSL for Requirement R3 should capture not documenting the absence of lessons learned. The SDT agrees and has made this change.

One commenter proposed to replace the Requirement R3 VSLs with graduation from 90-210 days beyond the required obligation. The SDT agrees and has made this change.

One commenter noted the graduation of VSLs for requirement part 2.2 incorrectly lists a period of within 19 calendar months for the Severe category, and the SDT has modified this to be 18 calendar months.

QUESTION C12 – CIP-010-1:

If you disagree with the changes made in CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-010-1 expressed in comments were (1) references to CIP-005, CIP-006, and CIP-007 within CIP-010, (2) scope of baseline configuration items in R1.1, (3) applicability including associated assets/systems and also including "external routable connectivity" language, (4) requirement language above and beyond FERC Order 706, and (5) other requirement and measure language modifications. The sections below are a summary of the comments received and include SDT responses for CIP-010-1.

CIP-010-1 General Comments

Many commenters requested an explanation for why CIP-010 depends on CIP-005, CIP-006, and CIP-007. Based on previous requirements in older versions of CIP-003, CIP-005, and CIP-007 (CIP-006 has since been removed from requirement language), the SDT combined the various requirements related to configuration change management and vulnerability assessments to create CIP-010. Both configuration change management and vulnerability assessment require validation that controls from CIP-005 and CIP-007 are not affected. Therefore, CIP-010 references CIP-005 and CIP-007. The SDT does not believe this cross-referencing creates a "double jeopardy" situation. Whether the requirement existed in CIP-005 or CIP-007, if an issue is discovered, then the issue would be a violation of where the requirement was enforced (CIP-005 or CIP-007) rather than in the requirement which enforced the search for issues (CIP-010). New "identify, assess, and correct deficiencies" requirement language will also aid in compliance concerns.

Several commenters mentioned that they desired a return to the approved language in CIP-003-4 Requirement R6 and CIP-007-1 Requirement R1 with targeted and efficient changes to address the FERC order. Another commenter further recommended a return to the draft 1 language. The SDT disagrees with their determination and believes that the current CIP-010-1 language is proper and in order. Based on this commenting period, the SDT has revised language for clarity and consistency. Language was also modified in an effort to address industry comments.

Numerous commenters recommended that all references to Medium Impact BES Cyber Systems in CIP-010 applicability include: "with External Routable Connectivity." The SDT does not agree with the addition of External Routable Connectivity to CIP-010 applicability. Whether a cyber asset has some type of connectivity or not, it can still be pervious

to vulnerabilities (i.e., Stutnex). The SDT's determination is in accordance with FERC Order 761, Paragraph 86. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010.

One commenter proposed removing from the measures: "… and the output of the tools used to perform the assessment," since this is thought to be a part of CIP-010-1 Requirement R3.4. The SDT does not agree with this modification since CIP-010-1 Requirement R3.4 asks for the results of the assessments, while CIP-010-1 Requirements R3.1 through R3.3 are referring to the output of any tools used to perform the assessment. In consideration of this comment and other industry comments, the SDT included "any" to the requirement in the case that no tools were used to perform the assessment.

Several commenters suggested the removal of: "… but not limited to …" in CIP-010 measures. The SDT has modified measure language in consideration of their comment. The SDT also emphasizes that the: "… but not limited to …" is supposed to benefit the responsible entity and not create an item for auditors to use against them.

Multiple commenters suggested that specific controls from CIP-005 and CIP-007 be identified in CIP-010-1 Requirements R1.3, R1.4.1, and R3.1 so there would be no need for interpretations. These comments were taken into consideration, and the related requirement sub-parts were modified accordingly. The references to CIP-005 and CIP-007 were removed from some requirement sub-parts. Also, per consideration of these comments, CIP-006 was removed from requirement language where the language was present.

One commenter believed that some requirements in CIP-010 expand the scope and documentation burden beyond earlier CIP standards versions due to CIP-005 and CIP-007 references. In consideration of these comments, the SDT has modified CIP-010-1 Requirements R1.3 and R3.1 accordingly. References to CIP-005 and CIP-007 have been removed from the sub-part requirement language. It should be noted that the SDT disagreed to removing these references in Requirement R1.4.1. The SDT also added the reference to Requirement R1.5.1 for consistency across Requirement R1.

One commenter recommended adding a reference to the associated requirement part in which each CIP-010-1 VSL is related. The VSLs are written at the higher-level requirement, but do include elements that refer to the various requirement parts. Therefore, the SDT does not believe that the associated requirement part needs to be included in the VSL. One commenter continued to suggest that the VSL language should more closely mirror the requirement language. The SDT has taken into consideration this comment and modified the VSL language accordingly.

One commenter mentioned that having a documented baseline and monitoring it closely makes the vulnerability assessment prior to deployment have no benefit. The SDT does not agree with this assessment, as a vulnerability assessment is more than just monitoring for changes to the baseline. Please see the guidelines section of the standard for CIP-010-1 Requirement R3. Also, other commenters mentioned that establishing a production-like environment that could produce an active vulnerability assessment would be difficult and expensive. The SDT added the language: "… production environment where the test is performed in a manner that minimizes adverse effects …" for instances when a test environment is not available.

One commenter recommended an expanded glossary of the many terms used in CIP-010. The SDT has taken this comment into consideration and has expanded upon the guidelines to include more guidance around terms related to the baseline configuration and cyber security controls.

One commenter recommended further items to be incorporated into the baseline configuration; including communication protocols, non-standard BIOS configurations, and other items. The SDT believes that the requirement language is sufficient as written, as adding additional items into the baseline configuration at this time period would be difficult to support consensus.

One commenter recommended that CIP-010-1 have an effective date that is 12 months after the effective date of the CIP V5 standards. The SDT will take this comment into consideration, as this comment references the Implementation Plan and not necessarily language within the CIP-010-1 standard.

One commenter commented on the use of the term "Configuration" versus "configuration." The SDT has revised CIP-010-1 to only use "configuration," since it was not the SDT's intent to include "Configuration," as this is not a NERC defined glossary term. Furthermore, another commenter questioned if the terms: "configuration management," "configuration change management," and "asset management" were synonymous terms. The SDT has revised CIP-010-1 to only use "configuration change management" for less confusion. "Asset management" is not synonymous with the other words in the previously mentioned sentence. "Asset management" where it is used (R1.1 measures) refers to SAP, Maximo, Cascade, Passport, or other asset management software. Also, due to other questions around the baseline configuration, the SDT has added further guidance to aid in entities' development of their baselines.

Applicability Section

A couple comments mentioned that the exemption language in Section 4.2.4 should be changed back to the previous ballot's CIP-010-1 language or this section should be struck if it truly only applies to CIP-002-5. The difference between the initial ballot posting and successive ballot posting is 4.2.3.5, which states that: "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes."

One commenter recommended the striking of the applicability component of the main requirement. If the commenter is referring to Section 4 of CIP-010, then this section is required for NERC standards to identify the standard's applicability to Responsible Entities, while the (newly termed) "applicable systems" columns in the tables refers to the scope of systems to which a specific requirement row applies.

Many commenters recommended removing some or all associated assets/systems from various applicability sections in the CIP-010 requirements because they represent an increase in scope from CIP V3/V4. The SDT disagrees with this assessment, as CIP Version 3 and Version 4 standards mention applicability to cyber assets within the ESP. The cyber assets that could exist within an ESP would include Associated Protected Cyber Assets, Associated Electronic Access Control or Monitoring Systems, and Associated Physical Access Control Systems. Therefore, the SDT does not believe that the assets/systems from CIP-010's applicability represent an increase in scope from CIP Version 3 and Version 4 standards.

One commenter expressed concern over 4.2.2, bullet 3, which references: "… Transmission where the Protection System is required by a NERC or Regional Reliability Standard." The concern was that CIP-010-1 was requiring the installation of a Transmission Protection System. This assessment is incorrect. CIP-010-1 does not require the installation of a Transmission Protection System, but other NERC or Regional Reliability Standards may require the installation of a Transmission Protection System.

Guidelines Section

Several commenters suggested adding the phrase: "network connectivity to identify" to the Requirement R3 guidance with regard to passive network discovery. The standard has been modified in consideration of these comments to include the phrase. One commenter made several other suggestions (such as the addition of details on baseline configurations and cyber security controls) in regards to guidance that informed the SDT's modification of that section.

Background Section

Several commenters mentioned that the third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. The SDT believes that this third paragraph is clear in stating:

- A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.
- The word "required" is not used to describe numbered or bulleted lists. The SDT wishes to emphasize that measures are only examples of evidence.

Requirement R1

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has added the "in a manner that identifies, assesses, and corrects deficiencies" language to the requirement, which is described above.

One commenter proposed that the requirement be changed to a program- or performance-based level to allow more flexibility (citing FERC FFT Order, Paragraph 81). The comment furthermore mentions that programs such as Tripwire would not be able to be used. Other commenters had similar comments in regards to the prescriptive language of CIP-010-1 Requirement R1.1. Based on the revised "identify, assess, and correct deficiencies" language, the SDT believes that more flexibility is achieved through an entity's internal controls process. Furthermore, the SDT believes that programs such as Tripwire could be used to aid in compliance with CIP-010-1 Requirement R2.

One commenter believed that information in Requirement R1 should only be collected for personal computers and protective relays. The SDT disagrees with this comment, as the applicability should involve all BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems since these assets can be found within the same Electronic Security Perimeter.

One commenter asked if recording software "hashes" can be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset. The SDT attempted to provide flexibility to allow the entity to determine how to track changes. However, in regards to CIP-010-1 Requirement R1, the baseline configuration still must be documented. If an entity is able to use software "hashes" to monitor for changes to the baseline configuration of a BES Cyber System, then this solution could be used for CIP-010-1 Requirement R2.1.

One commenter proposed a modification to language in CIP-010-1 Requirement R1 to eliminate the term "baseline" so that it is not confused with the security baselines that they create today for devices. Two other commenters also wanted to remove the "baseline" from CIP-010-1 requirement language. The SDT disagrees with the proposed change and believes that the language, as is with the term "baseline," is sufficient.

Requirement Part 1.1

A few commenters emphasized that Version 4 did not apply to noncritical; but in accordance with FERC Order 761, Paragraph 86, these assets/systems should be included in CIP-010-1 Requirement R1.1. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010-1 Requirement R1.1. Numerous commenters also alternatively recommended that CIP-010-1 Requirement R1.1 applicability only include High Impact BES Cyber Systems. The SDT disagrees and continues to cite FERC Order 761, Paragraph 86.

Several commenters disagreed with the use of the phrase: "… each Cyber Asset identified, individually or by group." The SDT has revised the requirement language in regards to their comment so as to ensure baselines can be defined at the individual or group level.

One commenter also desired a clarification of what may be grouped under CIP-010-1 Requirement R1.1. The SDT hopes that the revised requirement language provides additional clarity.

Requirement Part 1.1, Sub-Part 1.1.1

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Several commenters recommended replacing "exists" with "is either operating or running." Another commenter believed the wording of "is installed" is also sufficient. The SDT wants to underscore that "exists" refers to the case when an asset has firmware instead of an Operating System.

Requirement Part 1.1, Sub-Part 1.1.2

One commenter mentioned that "BES Cyber Asset" should be replaced with "applicable Cyber Asset." Other commenters had a similar position with regards to the use of "BES Cyber Asset." These comments were taken into consideration and

the related requirement sub-part was modified. The phrase “on the BES Cyber Asset” was removed from the requirement sub-part for consistency.

Multiple commenters requested clarification on the “applications.” Does “applications” mean “SCADA, EMS, State Estimator, etc.” instead of “device drivers and DLL applications” included in an operating system or package?” In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

A couple commenters suggested the removal of the word “intentionally” from the requirement language. The SDT believes that the use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for cyber asset use should be included. It is not the SDT’s intent for notepad, calculator, DLL, device drivers, or other applications included in an operating system package to be considered as commercially available or open-source application software. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities requested clarity on how granular the version identifier should be. The SDT provides flexibility for entities to determine what version levels should be tracked. The purpose of tracking the version allows entities to keep abreast of the version levels in their inventory. If software manufacturers alert entities to vulnerabilities in their software, the affected population could be identified through software version. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities suggested that sub-part 1.1.2 should exclude anti-malware signature file version identifiers due to the volatility of frequency updates. The SDT believes that only version levels that can aid in recognizing affected software should be tracked. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Requirement Part 1.1, Sub-Part 1.1.3

Multiple entities asked if a version control tool/system (like Concurrent Versions Systems) could demonstrate the custom software's version. In consideration of these comments, this requirement sub-part has been reworded to be "custom software installed." However, even in its successive ballot form, the requirement sub-part did not require the custom software version. Instead, the requirement sub-part requires the identification of the custom software.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Multiple commenters suggested removing "developed for the entity." The SDT has taken this comment into consideration and modified the requirement language accordingly.

There were several commenters who proposed modified language to clarify the term "custom software." The SDT disagrees with these proposed changes, but has reworded the requirement language in an attempt to provide additional clarity.

Requirement Part 1.1, Sub-Part 1.1.4

There were many commenters who believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what patches should be installed, while CIP-010 handles the patch being implemented (i.e., going through the configuration change management process).

One commenter believed that CIP-010-1 Requirement R1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Only ports which are accessible need to be included in the baseline. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter asked for clarity around "logical network accessible ports." In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter mentioned that the applicability columns from CIP-007 should match the applicability column in CIP-010-1 Requirement R1. The SDT does not agree with this comment, as the concept in CIP-010 is to identify logical network accessible ports, while CIP-007 requests entities to enable logical network accessible ports.

Requirement Part 1.1, Sub-Part 1.1.5
One commenter mentioned that CIP-010-1 Requirement R1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. This comment was taken into consideration and the related requirement sub-part was modified.

Many commenters believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what should be used, while CIP-010 is the implementation.

One commenter believed that CIP-010-1 Requirement R1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. Only historic or current patches that have been applied would be included in the baseline.

Several comments raised the concern Requirment R1.1.5 changes too frequently to be in the baseline and should be removed; that the evaluation of each patch is already included in CIP-007-5. The SDT believes that CIP-010-1 Requirment R1.1.5 is supposed to be a comprehensive listing of the patches that have been installed on the device. Patches are not required to be evaluated with this requirement. Instead, if a patch has been added to the device, then an update of the baseline is required.

Measures for Requirement Part 1.1
Per a comment, “or group” was added to CIP-0101 Requirement R1.1 measures to make consistent the requirement language and measures.

Requirement Part 1.2
One commenter proposed a rewording of CIP-010-1 Requirement R1.2 to: “Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware.” The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP Version 5 requirement language.

One commenter proposed indicating the appropriate authorizing individual or delegate in the requirement. The SDT believes that the requirement is sufficient, as is since it provides flexibility so that the entity can select the appropriate authorizing individual.

Measures for Requirement Part 1.2

One commenter recommended the removal of language in measures around individuals or groups with the authority to authorize the change. The SDT believes that measures are only examples of evidence. To be in compliance with the requirement language, an entity could authorize change by an individual, a group, or other entity-determined method.

There were two comments that recognized a concern with the language: "Documentation that the change was performed in accordance with the requirement." There was another suggestion to remove this language since it is not clear to what term the requirement is referring. The SDT believes that since the measure is for CIP-010-1 Requirement R1.2, that the language in the measure directly refers to CIP-010-1 Requirement R1.2 language only. While the SDT considered adding a reference to CIP-010-1 Requirement R1.2 in the measure to make explicit the requirement to which the measure language was referring, for consistency across CIP-010, this change was not made.

Requirement Part 1.3

One commenter mentioned that the applicability columns from CIP-005 and CIP-007 should match the applicability column of CIP-010-1 Requirement R1.3. This comment was taken into consideration and the related requirement sub-part was modified accordingly. The reference to CIP-005 and CIP-007 was removed from the requirement sub-part; and, therefore, the applicability columns between the standards do not need to be consistent.

There were many commenters that expressed concern with the 30-day time frame. Other commenters recommended the removal of the 30-day time frame for updating the baseline configuration. The SDT disagrees with the commenters and believes that a 30-day time frame allows entities time to update their baseline configuration documentation. Similiarly, other commenters had issues with the 30-day time frame and the references to CIP-005 and CIP-007. These issues are no longer a concern, as the SDT has removed the reference to CIP-005 and CIP-007 in regards to the 30-day time frame.

Two commenters were concerned about 'triple', or 'double' jeopardy with CIP-005 and CIP-007. One commenter suggested a revision or removal of the references, while another suggested that the requirement be moved to CIP-005 or CIP-007. In consideration of their comment, the SDT has modified CIP-010-1 Requirement R1.3 accordingly. In response, references to CIP-005 and CIP-007 have been removed from the sub-part requirement language.

Requirement Part 1.4

Many comments stated that "High Impact BES Cyber Systems" should be removed from applicability in CIP-010-1 Requirement R1.4 since this requirement sub-part is repetitious with CIP-010-1 Requirement R1.5. While CIP-010-1 Requirement R1.4 has been modified due to comments from industry, the SDT disagrees that CIP-010 Requirement R1.4 is repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

A bevy of commenters believed that this requirement should include an exclusion for CIP Exceptional Circumstances. The SDT does not agree with this comment, as even after the CIP Exceptional Circumstance has happened, an entity should determine that controls were not adversely affected.

Several commenters suggested that guidance be added on cyber security controls. The SDT has taken their comment into consideration (in addition to other similar inquiries on cyber security controls) and added additional information on cyber security controls in CIP-010 guidance.

One commenter proposed the following language for this requirement part: "For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007, [do 1.4.2]." While the SDT considered this approach, the SDT believes the current requirement language is sufficient as is.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.1

One commenter suggested a language change of "determined" to "identified." The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed CIP-010-1 Requirement R1.4.1 where "could be impacted" is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where "could be impacted" is a remote possibility. Southern believed that documenting "what could be impacted" is not a reliability benefit, it's the verification that controls are not affected by a change. The SDT agrees with their recommended change, and the requirement language has been updated accordingly in Requirement R1 with: "implement, in a manner that identifies, assesses, and corrects deficiencies," to avoid the zero-defect audit enforcement concern.

Several commenters believed that CIP-010-1 Requirement R1.4.1 could result in the Responsible Entity declaring that no cyber security controls are expected to change and, thus, no testing is required. The SDT does not agree with this assessment, as the requirement requires documentation of what could be changed followed by verification that potentially impacted controls were not affected in CIP-010-1 Requirement R1.4.2.

Many commenters recommended the removal of Requirement R1.4.1. The concept is that an entity identifies all related controls that could be impacted based on all requirements in CIP-005 and CIP-007. Therefore, the SDT believes that by mentioning CIP-005 and CIP-007, there is no need for interpretations. In fulfilling the requirement, an entity must identify that a particular change impacts CIP-005-5 Requirement R1 or CIP-005-5 Requirement R1 and CIP-005-5 Requirement R2. If all requirements in CIP-005 and CIP-007 may be affected by a deviation to the existing baseline configuration, then this would be documented in accordance to CIP-010-1 Requirement R1.4.1. It should also be mentioned that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.2

One commenter mentioned that “BES Cyber Asset” should be replaced with “applicable Cyber Asset.” This comment was taken into consideration and the related requirement sub-part was modified. The phrase “BES Cyber System” was removed from the requirement sub-part for consistency.

Many commenters expressed concern with CIP-010-1 Requirement R1.4.2’s “availability” term. The SDT has modified the requirement language in consideration of these comments. The “available” term has been removed.

One commenter proposed that the word “determined” be changed to “identified.” The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed the term “applicable” should be added for clarity. The SDT remarks that “applicable” is not required, as CIP-010 Requirement R1.4.2 points to CIP-010-1 Requirement R1.4.1, which ensures entities only look at the potentially impacted controls.

One commenter requested clarification of use of the term "required controls." The word required refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. While the SDT references all of CIP-005 and all of CIP-007, CIP-010-1 Requirement R1.4.1 requires entities to identify those controls in CIP-005 and CIP-007 that are potentially impacted. Therefore, CIP-010-1 Requirement R1.4.2 is only looking at the controls identified in CIP-010-1 Requirement R1.4.1.

One commenter proposed the addition of a time frame for how long an entity may take to make the verification required in CIP-010-1 Requirement R1.4.2. The SDT has taken this into consideration. The SDT also believes that the "identify, assess, and correct deficiencies" should provide aid in compliance concerns regarding this requirement.

CIP-010-1 Requirement Part 1.5, Sub-Part 1.5.1

Multiple commenters expressed concern with the language in CIP-010-1 Requirement R1.5.1. A few of the aforementioned organizations mentioned that the parenthetical expression in CIP-010-1 Requirement R1.5.1 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered. Other organizations recommended changing CIP-010-1 Requirement R1.5.1 language to: "testing cyber security controls, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. The SDT has reworded requirement language based on industry comment and hopes that the changes provide additional clarity. Alternatively, other organizations proposed the removal of the following language in CIP-010-1 Requirement R1.5.1: "…that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT disagrees with the comment, as documenting the differences between the test and production environment is a completely separate task compared to modeling the baseline configuration. Modeling the baseline configuration is an attempt to re-create the baseline configuration on a single asset, while documenting differences between the test and production environment would simulate the rest of the assets in that environment and how they function together. Other organizations were concerned that the revised language in the posted standard removed the possibility for a technical feasibility exception. The SDT does not agree, as old, legacy systems may not be available in a test environment and there may be no way to utilize a production environment where a test can be performed in a manner that minimizes adverse effects.

One commenter asked if this requirement interferes with CIP-010-1 Requirement R1.4 for High Impact Systems. There was a suggestion to remove the overlap in applicability of the two requirements and adding clarifying language as to

what is intended and required in CIP-010-1 Requirement R1.4 vs. CIP-010-1 Requirement R1.5. The SDT wishes to underscore that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 R1.5. CIP-010-1 R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

One commenter requested clarification of use of the term: "required controls." The SDT responds by claiming that "required" refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. Additional information on cyber security controls were added in CIP-010-1 Guidelines for Requirement R1.

Several commenters expressed concern over the "where technically feasible" language. Alliant Energy proposed that: "where technically feasible" should be changed to "where test environments exist." One commenter wanted to know what the language pertained to. The SDT does not agree with the proposed modification. The language in the requirement allows for test environments to exist in a production environment where the test is performed in a manner that minimizes adverse effects. Also, it should be made clear that the exception language refers to both CIP-010-1 Requirement R1.5.1 and Requirement R1.5.2.

Requirement Part 1.5, Sub-Part 1.5.2

Some commenters believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." Another commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important.

SPP RE and City Utilities of Springfield, MO asked if CIP-010-1 Requirement R1.5.2 permits the documentation of a stand-alone test environment with identified differences from the production environment. The SDT concurs that the requirement language requests documentation of the differences between the test and production environment, if a test environment was used. If the differences did not change from change to change, then the same documentation would be included with each change package that is processed.

Requirement R1 VRFs

Based on numerous comments, the VRFs in Table of Compliance Elements now match the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirement R1 and Requirement R2.

Requirement R1 VSLs

There were two commenters who suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. The SDT will take this into consideration, as we apply the non-zero defect forward looking compliance process.

Two commenters suggested that "any" be changed to "one or more" in the High VSL for CIP-010-1 Requirement R1. The SDT has updated the VSL language per the comment's recommended change.

One commenter believed that the phrase "and to document those changes" in the first condition of the High VSL for CIP-010-1 Requirement R1 should be deleted, as it is duplicative of the second condition. The SDT has removed the second condition due to modification to the requirement language to remove reference to other CIP standards in CIP-010-1 Requirement R1.3.

Main Requirement R2

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

Requirement Part 2.1

Many comments were on the initial ballot posting language, as the successive ballot posting language is not understandable. The SDT has modified the requirement in consideration of their comment.

One commenter believed that double jeopardy exists with CIP-010-1 Requirement R1 and CIP-010-1 Requirement R2.1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under CIP-010-1 Requirement R1, not a separate requirement. The SDT disagrees with this assessment. CIP-010-1 Requirement

R2.1 does not create a double jeopardy situation with CIP-010-1 Requirement R1 since the violation would be in CIP-010-1 Requirement R1, not in CIP-010-1 Requirement R2.1. CIP-010-1 Requirement R2.1 requires entities to document and investigate detected unauthorized changes. If one of the unauthorized changes is due to a violation of CIP-010-1 Requirement R1, then the self-report would be on CIP-010-1 Requirement R1 and not on CIP-010-1 Requirement R2.1. However, based on the new "identifies, assesses, and corrects deficiencies" language, if an issue is detected, based on an entity's internal control processes, this would not be a self-report. Other commenters stated on CIP-010-1 Requirement R2 creating a situation where a need would exist to self-report. With the new requirement language of "identifies, assesses, and corrects deficiencies," a self-report would not be necessary.

Many commenters essentially mentioned concerns centered on technical feasibility language. Some of the aforementioned organizations requested that the term "continuous" be removed from requirement language; while others proposed language that would remove the technical feasibility exception. The SDT has modified the requirement language in consideration of these comments. One commenter further commented that the language should be revised in such a way that only devices that can monitor automatically should be included; otherwise, a technical feasibility exception should be allowed. The SDT has modified the language such that monitoring could be done manually or continuously depending on the device.

One commenter suggested a change to the following language: "Document changes tracked through the entity's change management program." The SDT does not agree with this approach and believes the language is sufficient as is. One commenter recommended a similar approach of modifying the language due to their desired removal of "baseline" term use.

Many commenters suggested a different time frame for monitoring. The suggestion called for a 90-day instead of 35-day time frame, while other commenters suggested an annual or quarterly time frame. The SDT believes that a 35-day time frame is sufficient for an "express acknowledgement."

One commenter believed that the requirement will be burdensome and nothing gained from it except a lot of TFE paperwork to track. The SDT disagrees with this comment, as the requirement was added based on FERC Order 706.

One commenter asked if no change is detected during a monitoring period, how an entity can demonstrate that "no change" occurred. The requirement language mentions that only detected unauthorized changes need to be documented and investigated. If there is no change, then this would not need to be documented.

Measures for Requirement Part 2.1
One commenter emphasized that the requirement requires monitoring for all changes, yet the measure mentions calls for investigation of any unauthorized changes. They believe that the requirement language should be changed to include "unauthorized" changes such that monitoring is only necessary for unauthorized changes. The SDT does not agree with this assessment and believes that the requirement language and measures are sufficient as is.

One commenter requested clarity on the phrase "record of investigation." "Record of investigation" would be some type of documentation that shows that a detected unauthorized change was documented and investigated accordingly.

Requirement R2 VRFs
Multiple commenters stated that the VRFs in the table of compliance elements now matches the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R2 VSLs
Several commenters suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: "severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention." The SDT will take this into consideration as we apply the "non-zero defect forward looking compliance process."

Two commenters believed that a new gradated VSL should be introduced due to time-period language added in the previous posting. The SDT has taken this comment into consideration. While gradated VSLs were not introduced, since the requirement language includes "… identify, assess, and correct deficiencies…", the VSLs have been updated. .

Requirement R3
One commenter proposed a revision to Requirement R1 to read: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

A few commenters mentioned that the applicability between CIP-010-1 Requirements R3.3 and R3.4 differed. The SDT recognizes this difference and emphasizes that these are two different requirements and, hence, the applicability should be different.

One commenter asked if all Vulnerability Assessments under Requirement R3 must be performed prior to Version 5's Effective Date or whether entities have an additional year or three years from the effective date. The answer to NIPSCO's question can be found in the CIP Version 5 Implementation Plan. CIP-010-1 Requirements R3.1 and R3.2 must initially be complied with 12 months after the Effective Date of the CIP Version 5 standards.

One commenter asked why CIP-010-1 Requirement R3 does not always include Medium Impact in its scope. The SDT believes that the applicability as is can be considered sufficient. TRE also had concerns that the Requirement R3 does not include an annual vulnerability assessment. This is incorrect as CIP-010-1 Requirement R3.1 requires an annual vulnerability, while CIP-010-1 Requirement R3.2 requires a 36-month vulnerability assessment (for the applicable systems).

One commenter asked for clarity over the inclusion in applicability of Electronic Access Control or Monitoring Systems in CIP-010-1 Requirement R3. This requirement has the same applicability for these systems as in previous NERC CIP version. Therefore, the SDT believes that these systems should remain included in the applicability for CIP-010-1 Requirement R3.

One commenter asked if vulnerability assessments are required for every cyber asset or a sampling of cyber assets. Per applicable systems section, the vulnerability assessment is required for the systems listed.

Requirement Part 3.1

Commenters recommended that the requirement start with its purpose. The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP V5 requirement language.

Many commenters proposed to reword Requirement R3.1 with the following language: "once each calendar year or a period not to exceed 15 calendar months between assessments." The SDT has taken these comments under consideration and is modifying the requirement sub-part language accordingly. One commenter proposed alternative language allowing an entity determined time frame. The SDT disagrees with this comment since the 15 calendar months' time frame is sufficient.

A few commenters believed that double jeopardy exists with reference to CIP-005, CIP-006, and CIP-007. The SDT does not agree, as if controls are not implemented correctly, then this would be a violation in the respective CIP standard, and not CIP-010-1.

Many commenters recommended that CIP-006 be removed from requirement language. The SDT agrees and has removed the reference to CIP-006.

Multiple commenters had concerns on what exactly constituted an active vulnerability assessment. The SDT points to guidance in CIP-010 on Requirement R3 in regards to recommended elements of an active vulnerability assessment. Also, other commenters asked if an active vulnerability assessment must be done for all systems or a representative sampling. Per the applicable systems section of the table for Requirement R3, the active vulnerability assessment must be done for all applicable systems.

One commenter requested clarification on whether an external vendor needs to perform the annual vulnerability assessment or can the Responsible Entity perform this task. The SDT provides enough flexibility in the requirement so that the RE can determine the solution that best meets its needs.

Several commenters believed that CIP-010-1 Requirement R3.1 is redundant with CIP-010-1 Requirement R1.3. The SDT does not agree, as CIP-010-1 Requirement R3.1 requires an annual vulnerability assessment, while CIP-010-1 Requirement R1.3 requires an update of the baseline configuration for a change that deviates from the existing baseline configuration.

Measure for Requirement Part 3.1
One commenter believed that reference to “individuals” in the first bulleted item needs to be removed. The SDT emphasizes that measures are only examples of evidence. However, the SDT has modified the measure language in consideration of the comment.

Requirement Part 3.2
Many commenters expressed concern with the language in CIP-010-1 R3.2. Another comment mentioned that the parenthetical expression in CIP-010-1 R3.2 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been

altered. Furthermore, the commenters recommended that this requirement start with its purpose. The SDT disagrees with these comments as the requirement language is consistent with other similar CIP Version 5 requirement language.

Multiple commenters asked for clarification on CIP-010-1 Requirement R3.2 in regards to this being a paper exercise. The requirement language mentions active vulnerability assessment. In response, please see the guidance section on additional details on an active vulnerability assessment.

Multiple commenters proposed the removal of the language: "that models the baseline configuration to ensure that required cyber security controls are not adversely affected" in CIP-010-1 Requirement R3.2, commenting that it is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT does not agree with this assessment. CIP-010-1, Requirement R3.2.1 requires performing an active vulnerability assessment in an environment that models the baseline configuration of the BES Cyber System in a production environment, while CIP-010-1 Requirement R3.2.2 requires documenting the results of testing, and if, a test environment was used, documenting the differences.

One commenter asked how is this requirement differs from CIP-007. The SDT remarks that CIP-010-1 Requirement R3.2 is related to completing a vulnerability assessment every three years to assess controls in CIP-007 (and CIP-005) are implemented correctly.

One commenter believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." One commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important in establishing how the testing environments differ.

A few commenters asked if the assessment in CIP-010-1 Requirement R3.2 is in lieu of or in addition to the assessment required by CIP-010-1 Requirement R3.1 in the calendar year that the CIP-010-1 Requirement R3.2 assessment is conducted. The SDT believes that CIP-010-1 Requirement R3.2 is in lieu of CIP-010-1 Requirement R3.1 in the calendar year that CIP-010-1 Requirement R3.2 is conducted.

One commenter asked if CIP-006 is within scope of CIP-010-1 Requirement R3.2. The SDT has removed the reference to CIP-006 in CIP-010-1 Requirement R3.1, and is not a similar reference in CIP-010-1 Requirement R3.2.

One commenter proposed that the phrase: "where technically feasible" should be changed to "where test environments exist." The SDT does not agree with this modification since language in the requirement allows for "test environments" to exist in a production environment where the test is performed in a manner that minimizes adverse effects.

There was a comment mentioned that CIP-010-1 Requirement R3.2 requires assessments every three years, while CIP-007-3 Requirement R8 required vulnerability assessments annually. It was thought that we weakened the requirement; however, CIP-010-1 Requirement R3.1 requires an annual vulnerability and, therefore, the annual requirement in CIP-007-3 Requirement R8 was not weakened.

A commenter requested that associated electronic access control or monitoring systems and associated protected cyber assets should be added to the applicability for Requirement R3.2. For consistency in CIP-010-1, the SDT does not agree with the proposed change in applicability.

Requirement Part 3.3

One commenter believed it to be problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. The SDT acknowledges the concern, but emphasizes that an active vulnerability assessment is not required in the cases of a CIP Exceptional Circumstance or like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset.

One commenter believed that the term "active vulnerability assessment" is not defined. The SDT disagrees with this statement, as guidance is provided that aids in understanding an active vulnerability assessment. Furthermore, the commenter stated that since sufficient change management controls exist that an active vulnerability assessment is unnecessary. The SDT disagrees with this statement, as the configuration change management controls in CIP-010-1 Requirements R1 and R2 are in place for changes that deviate from the existing baseline configuration, while vulnerability assessments in CIP-010-1 Requirement R3 are for ensuring proper controls and detecting vulnerabilities.

One commenter mentioned that the parenthetical expression in CIP-010-1 Requirement R3.3 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered.

Multiple commenters expressed concern around the language in CIP-010-1 Requirement R3.3. Some of the aforementioned organizations recommended that this requirement start with its purpose. Other organizations recommended a revision of the language. The SDT has taken these comments into consideration and modified the requirement language accordingly.

Multiple commenters suggested revisions to "prior to adding" language. One commenter proposed that instead of "prior to adding," that the requirement language should read: "before closing the change." Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

One commenter believed that the parenthetical explanation of a like replacement should be moved to guidance. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

Several commenters believed that CIP-010-1 Requirement R3.3 appears to be missing "and" after the parenthesis. Without the parenthetical, it should read "Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset..."

A couple commenters suggested that Physical Access Control Systems should be added in the applicable systems column. The SDT does not agree with their proposed change, as references to Physical Access Control Systems and CIP-006-1 have been removed throughout CIP-010-1.

One commenter expressed confusion around the use of the term: "new Cyber Asset." The commenter questioned if this term references a new Cyber Asset that is part of an existing Cyber System, or a new Cyber Asset per CIP-002. The SDT remarks that CIP-010-1 Requirement R3.3 is for new Cyber Assets with baseline configurations that do not currently exist. Therefore, a new Cyber Asset that is part of an existing Cyber System (and that has an existing baseline configuration) does not require an active vulnerability assessment per CIP-010-1 Requirement R3.3.

Several commenters believed that the language should be consistent among CIP-010-1 Requirements R3.1 through R3.3 in regards to vulnerability assessments. The SDT has modified the requirements accordingly in consideration of their comment.

A commenter asked if cyber assets can be placed in ESP before remediation of identified vulnerabilities. The SDT remarks that cyber assets can only be placed in ESP before remediation of identified vulnerabilities if a CIP Exceptional Circumstance exists or the cyber asset is a "like replacement."

CIP-010-1 Requirement Part 3.4

One commenter suggested that the term "if any" be added in CIP-010-1 Requirement R3.4 to denote the need to document the results of assessments that identified no vulnerabilities. The SDT disagrees as the language in CIP-010-1 Requirement R3.4 follows closely to the language in its previous instance in an earlier CIP standards version.

Many commenters expressed concern with the phrase: "remediate or mitigate vulnerabilities" and the related documentation. Another commenter proposed to replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. The SDT developed this requirement language directly from the previous CIP versions. The concept is that an entity must document how they plan to remediate or mitigate identified vulnerabilities. CIP-010-1 Requirement R3 becomes an internal controls requirement to ensure that cyber security controls are properly implemented. While other commenters asked if it is the intent that identified vulnerabilities would not constitute violations of requirements they are found against. It is not the SDT's intent that an identified vulnerability would not constitute a violation of other requirements. While CIP-010 would not be violated, the respective CIP-005 or CIP-007 standard may be violated. The SDT does believe that the self-report mitigation plan could be used as the action plan for Requirement R3.4.

Several entities believed that the deadline for documenting the results of the assessment and the action plan should be specified. They suggested a 30-day limit. Also, they suggested including levels of gradation for not meeting the 30-day limit. One commenter took a different approach and recommended that "planned date" be changed to "estimated time frame." The SDT believes that the requirement language is sufficient as is.

Several commenters believed that more specificity should be added around the term “assessments” in CIP-010-1 Requirement R3.4. The SDT has modified the language in consideration of these comments and the text: “conducted pursuant to Parts 3.1, 3.2, and 3.3” was added to the requirement language.

One commenter asked for clarity in regards to the phrase “planned date of completing the action plan.” Is this the completion of the formulation of the plan or the completion of the tasks within the plan? The SDT articulates that the planned date of completing the action plan is related to the completion of the tasks within the plan.

Requirement R3 VRFs

There were multiple comments on VRFs, and the VRFs in Table of Compliance Elements now matches the VRF as identified at the Requirements and Measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R3 VSLs

Several commenters believed that corresponding to the proposed revisions to the requirement statement that the VSLs should be revised to read: “severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.” The SDT has taken this comment into consideration as we applied the “identify, assess, and correct” approach; however, that language should not be included here. The reasoning behind this decision is due to the CIP-010-1 R3 Requirement’s indirect (mentioned in R3 Guidance) reference to CIP-005 and CIP-007. The related language would relate to the timely performance of completing a vulnerability assessment instead of identifying and correcting deficiencies which may be a part of the related CIP-005 and CIP-007 langauge (CIP-005 does not include this language in its requirements).

Several commenters proposed that the third condition in Severe VSL have the word “or” instead of “and.” The SDT has modified the language in response to their comment.

One commenter believed that the VSL does not address the 36-month timeline in CIP-010-1 Requirement R3.2. Furthermore, the commenter proposed additional language to address this timeline. The SDT has taken this comment into consideration and modified the VSL language accordingly.

QUESTION C15 – CIP-011-5:

If you disagree with the changes made in CIP-011-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, there were many global comments that related not only to CIP-011, but to all of the CIP standards.

Annual Requirements
Many commenters objected to the posted language referencing annual requirements. Several suggested alternative ways to express the frequency for an annual requirement. The SDT considered all of the recommendations and decided use the phrase "at least once every 15 calendar months" (or similar) to express the frequency for annual requirements.

Use of the phrase "but not limited to" in measures language
The SDT received many comments objecting to the phrase "but not limited to" within the measures. Some comments suggested removal of the term; others recommended a default to the use of the word "or," while others suggested the use of the word "and." Commenters believed that using the "but not limited to" language creates confusion about whether the specified measures are necessary or sufficient. The SDT has considered this issue carefully. The SDT has modified the language to "examples of acceptable evidence include, but are not limited to." The phrase "but not limited to" is designed to be of benefit to the Responsible Entity, not be a back door "gotcha" for auditors. Use of the phrase allows the entity flexibility in the type of evidence they are able to provide both now and in the future.

Applicability Column Title
The length of the applicability column title caused confusion about the systems/assets that are within scope for some entities. Several commenters suggested shortening the column heading to "applicability." The SDT recalls that the title of the column as previously posted was in response to comments from the first posting. SDT has renamed the column "applicable systems."

The SDT received many comments stating that: "Medium Impact BES Cyber Systems should be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP Version 4 standards." A main goal of the SDT is to implement the FERC directives in Order 706 and Order 761. Order 761 states that FERC: "…supports the elimination of the blanket

exemption for non-routable connected cyber systems…continued blanket exemption in Version 5 would not adequately address risk." The SDT has considered each requirement concerning handling the exemption for non-routable connections. The SDT does not agree that in CIP-011 the scope should be limited to only BES Cyber Systems with External Routable Connectivity, as recommended in some comments.

Many commenters requested the removal of all references to systems and assets in requirements and that the SDT rely on the applicability column only to specify applicability. The SDT agrees with this recommendation. Wherever possible, the assets in scope will be indicated only in the applicability column. Several commenters suggested that the SDT remove all references to applicable assets in requirements and rely on the applicability column only to specify the Cyber Assets that are in scope. The SDT agrees. Wherever possible, the requirements have been streamlined to only reference applicable Cyber Assets within the applicability column.

Some commenters stated that the rationale for CIP-011 Requirement R1 was incomplete as originally posted. On May 8, 2012, NERC was alerted that the text contained in the rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete. NERC corrected this by issuing revised language that modified the text box size to display all of the text.

Some commenters recommended that entities should define their own info protection program. They suggested that compliance would be evaluated based on how the entity complied with their defined programs. The SDT discussed this comment, but disagrees. The SDT believes it would be doing the industry a disservice to leave the process completely up to the entity. As part of its change, the SDT seeks to clarify what is required to meet compliance. The SDT believes that if the requirements are not defined or entity defined, NERC will be forced to issue Compliance Application Notices in the future to provide clarity, and auditors will be forced to inject their own audit measurements. In the interest of providing clarity, the SDT believes it is important to provide a consistent threshold for compliance.

The SDT received comments asking that the team revert to legacy language used in previous versions of the CIP standards (V1 and V3). SDT considered this request, but believes that many entities have made good suggestions, which improve legacy language. Legacy language will be utilized in all cases where it is appropriate for the purposes of minimizing changes that the registered entities must make to their ongoing programs.

CIP-011 Requirement R1 calls for each Responsible Entity to implement an information protection program that includes applicable items, and Requirement R1.1 requires methods to identify such information. Many entities commented that Requirement R1.1 was too vague. In fact, several entities indicated they were confused as to whether the requirement

called for determining what information should be protected or if the requirement mandated labeling of the information. Some entities asked if specific classification was required. A few entities suggested that a specific classification, such as "confidential," should be included in the requirement. The SDT has considered this but does not believe it is appropriate to dictate a specific classification, such as "confidential." Some entities may use other classifications such as "CIP-Confidential," "Non-Public," "Highly Confidential," or many other designations. It is not the intent of the SDT to force all Registered Entities to modify their compliance documentation by mandating specific classifications. This initial part of the information protection program simply requires that the information in scope and to be protected is identified in some manner. Specific classification of information may be used as a method for identification, but is not specifically required. One commenter provided a specific recommendation to clarify that the information to be identified is that which is explained in the definition of BES Cyber System Information. The SDT agrees with this comment. The SDT is also responsive to industry comments and has enhanced the measures section of Requirement R1.

Some entities pointed out that the word "implemented" is unnecessary in the Requirement R1.1 requirement because it is contained in the overall Requirement R1 requirement language. They asked that the word "implement" be removed from Requirement R1.1 because it was redundant. Other entities stated that documentation is for measures or evidence, and the word "documented" should be removed from Requirement R1.1 requirement. The SDT has removed both "implemented" and "documented" from the requirement language. The term documented has been moved to the measures section.

There were additional comments related to the measures for Requirement R1.1. Some commenters asked how a repository could be a measure, and others asked for additional clarity. A repository could be a measure if the entity designated the repository or a section of the repository as the location for identifying and housing BES Cyber System Information and explained the protections afforded by the repository in the entity's Information Protection Program. It would be up to the entity to explain in their information protection program how the repository was used to identify their BES Cyber System Information.

In CIP-011 Requirement R1.2, many commenters again asked that additional clarification be added to the requirement concerning procedures for handling of BES Cyber System Information. The SDT agrees and has modified the requirement to clarify that handling procedures required are those which explain how the BES Cyber System Information is protected and secured.

Several comments asked for additional specifics concerning several topics regarding BES Cyber System Information; including transit, handling, and transmittal. The SDT agrees with this. The guidance section has been greatly expanded to address the topics requested.

Several entities desired additional specifics concerning the measures for Requirement R1.2. One entity commented: "This measure does not specify what records could be used …would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?" The SDT disagrees that it would serve the industry to mandate this level of specifics within CIP-011. It is the SDTs intent that the entities document their information protection program and associated procedures in accordance with the CIP-011 requirements, and that the entity maintains records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented program and associated procedures. A measure has been added which specifies this intent.

There were several comments requesting that the SDT address third party handling of BES Cyber System Information. The SDT agrees with this comment. Additional information has been added to guidance to cover this topic.

There were comments asking for more specifics concerning the topics of transit, handling, transmittal, distribution, physical access, purge, use, and disposal. The guidance section has been significantly enhanced to address the topics for which additional direction is warranted.

Some commenters recommended including procedures for reuse and disposal within Requirement R1. The SDT does not agree. SDT believes that the topic of reuse and disposal is complex and requires the specifics currently afforded the topic as specified in Requirement R2. If the topic was included in the Requirement R1 procedures, it could result in double jeopardy during audits, as auditors review compliance with Requirement R1 procedures and Requirement R2 handling during reuse and disposal.

Commenters stated that the reference to prior version under Requirement R1.2 refers to CIP-003-3, Requirement R5.3. They recommended that the reference be moved to Requirement R1.3. The SDT agrees.

The SDT received many comments related to Requirement R1.3. Many commenters recommended that the team specify that deficiencies found in the annual assessment should not be considered violations or potential violations. Some commenters asked that the SDT specify which deficiencies would be considered violations and which would not be considered violations. Commenters asked that the word "deficiencies" be changed to "lessons learned" or "flaws." The

SDT notes that the word “deficiencies” is appropriate because a deficiency notes there is a lack of completeness or insufficiency exists.

Some asked that the entire requirement be handled under the NERC FFT program and eliminated from the requirements. It is not up to the SDT to make the determination as to what is and what is not a violation. The SDT sought guidance from NERC and regional audit staff. The audit staff advised that some deficiencies could be seen as self-reportable violations or potential violations during audit if the entity failed to adhere to one of the specified sub-requirements. Other deficiencies might simply be process improvements or opportunities for improvements that do not violate any BES Cyber System Information sub-requirement from CIP-011. Further, the requirement calls for a periodic “assessment,” and such “assessment” may reveal things that went well in addition to things that could be improved. After considering industry comments and consulting with audit and NERC staff, the requirement will be handled under the Paragraph 81 project from the FERC Order on the find, fix, track and report process.

Some commenters did not like the grouping of all access control requirements within CIP 004. They asked that the requirement parts dealing with access to information be moved into CIP-011. This was discussed among the SDT. It was decided that the majority of entities favored the grouping of all access control within CIP 004. For consistency and in response to many previous comments, all access control requirements have been grouped into CIP 004. The requirement parts dealing with access control for BES Cyber System Information have, therefore, not been moved into CIP-011.

Some commenters asked where specifically the process covering reuse and disposal is required. Requirement R2 states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” Therefore, Requirement R2 requires the entity to define their process concerning the topics within Requirement R2.

The SDT received comments questioning a discrepancy between the types of systems referenced in the definition of BES Cyber System Information vs. the applicability column for Requirement R2. Associated Protected Cyber Assets is included in the applicability column, but is not specifically referenced in the definition. The SDT’s intent is that if BES Cyber System Information as defined in the standard exists in the data storage media of applicable Cyber Assets, then Requirement R2 applies.

One commenter pointed out that the component obligations under CIP-011-1 are not clear and that the table headers under Requirement R2 may be adding to the confusion, as they are different for Requirements R2.1 and for R2.2. The SDT agrees and has corrected the table headers so that they are consistent within Requirement R2.

The second paragraph in Requirements R2.1 and R2.2 that deal with removal of the device from the PSP generated many comments. Some commenters asked that the language concerning removal from the PSP be clarified. Others asked that the language be moved to a separate part. Others stated that the language adds no value and asked that the language concerning removal from the PSP be deleted from the requirement part altogether. A few commenters suggested simplified language, and such comments were very much appreciated. The SDT has decided to remove from the requirement language dealing with removal from the PSP. The SDT will address the topic of removal from the PSP within the guidance section. The SDT made corresponding changes to the measures section.

Many commenters objected to use of the term “chain of custody” in Requirements R2.1 and R2.2. They stated that this is a legal term, and they believe it is not appropriate in the CIP standards. Others commented that the intended use of the term “who has possession,” as used in the requirement, was unclear. The SDT has decided to remove the entire second paragraph from Requirements R2.1 and R2.2, including the reference to “chain of custody.” The SDT made corresponding changes to the measures section and any reference to terms such as “chain of custody” has been removed from the measures section, as well.

Some commenters recommended combining Requirements R2.1 and R2.2 into one requirement part. The SDT disagrees with this recommendation. SDT believes there are sufficient differences in the handling of release for reuse versus disposal to warrant retaining both Requirement R2.1 and Requirement R2.2.

Within the Requirement R2.1 language, some commenters asked for additional clarity concerning the exception, which provides for reuse within other high impact or medium impact BES Cyber Systems. The SDT agrees with this comment and has added additional clarity to the guidance language specifying that the re-use exception applies to re-use in other systems that are identified in the applicable systems column as protections will continue after re-use.

The SDT received comments asking that “BES” be inserted in front of “Cyber Assets” within the reference to “applicable Cyber Assets that contain BES Cyber System Information...” within Requirements R2.1 and R2.2. The SDT disagrees with this direction. The requirement parts are applicable to Associated Physical Access Control Systems, Associated Electronic

Access Control or Monitoring Systems, and Associated Protected Cyber Assets. Therefore, the scope of Cyber Assets which may contain BES Cyber System Information is larger than the suggested term "BES Cyber Assets."

The SDT received at least one comment stating that it was unclear if Requirement R2.2 meant the storage media within the Cyber Asset, or if it also includes backup media. The requirement states: "Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media." The SDT's intent is that the scope includes the Cyber Asset data storage media. The scope of this requirement is not far reaching to include all possible locations of downstream information, such as backup copies outside the Cyber Asset. However, such copies of BES Cyber System Information would be governed by Requirement R1.

Some entities also asked for additional specifics concerning the actions a Responsible Entity shall take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. One commenter questioned whether an attestation was specifically mandated. An attestation is not required by the standard. It is not the intent of the SDT to mandate specific actions within the requirements. However, the guidance section has been greatly expanded with guidance taken from NIST SP800-88, which provides additional assistance to entities.

One entity stated that it is not clear if requirement parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. The SDT considered this question and believes that the answer is: Yes, such actions would be permitted. The requirement calls for the entity to "take action to prevent unauthorized retrieval." This provides flexibility for the entity. As long as the entity documented the actions that they undertook; i.e., removing the media, securing the media, sanitizing the media in accord with the requirements, such action should be permitted.

SDT received the following comment: requirement part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contain BES Cyber System Information (i.e., network diagram). The second sentence appears to pertain to Cyber Assets within an ESP. There were other commenters asking for clarity concerning the storage media and the targets for sanitation in Requirement R2. Requirement R2 applies to any information within the Cyber Asset data storage media that meets the definition of BES Cyber System Information.

A few commenters stated that the standard needs to track the media and not necessarily the Cyber Asset the media is associated with. The SDT agrees with this comment. The Requirement R2 language has been modified to include the reference to "data storage media."

VSLs and VRFs

The SDT received at least one comment asking that the VRF for Requirement R1 be lowered. The SDT disagrees with the industry comment. The VRF for Requirement R1 is Medium in keeping with the FERC approved current VRF for this requirement. The VRF for Requirement R2 is already lower.

One commenter asked that the SDT add the "part" reference to the VSL so that the reader could easily understand the requirement number to which the VSL referred. The SDT agrees with this comment, and added the references to the VSL's.

Multiple commenters objected to the "zero defect" approach to VSL's for Requirement R2. The SDT agrees. The previously posted Requirement R2 VSLs have been modified to be less "device" specific. In the future, there will be additional emphasis on the entity providing good processes and security controls.

One commenter provided specific language for VSL's. Corresponding to recommendations that had been made concerning requirements, they asked that the VSLs should be revised to: Severe-not implemented, Higher-not measuring to detect, Moderate-not correcting detected flaws, Lower-not considering prevention. However, the requirement does not address prevention, and the VSLs must correspond to the requirements.

NERC will be sharing additional information on VRFs and VSLs in keeping with NERC's implementation of the FFT program.

Questions with Votes Only:

CIP-008, CIP-009, CIP-010 and CIP-011 Questions: Question 1

1. **CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Duke Energy	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No

Organization	Yes or No
NIPSCO	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No

Organization	Yes or No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Dairyland Power Cooperative	No

Organization	Yes or No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Springfield Utility Board	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review	Yes

Organization	Yes or No
Committee	
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Lakeland Electric	No

Organization	Yes or No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Utility Services Inc.	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces	Yes

Organization	Yes or No
Corporation	
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes

Organization	Yes or No
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
Puget Sound Energy, Inc.	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes

Organization	Yes or No
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Utility Services Inc.	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
PNM Resources	No
Arizona Public Service Company	No
Progress Energy	No
Hydro One	No
Tampa Electric Company	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Oncor Electric Delivery Company LLC	No
CenterPoint Energy	No
Xcel Energy	No
New York Power Authority	No
MidAmerican Energy Company	No
PJM Interconnection	No
ISO New England Inc.	No
ACES Power Marketing	No
Puget Sound Energy, Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Brazos Electric Power Cooperative	No
IRC Standards Review Committee	Yes
The united illuminating Company	Yes
Lakeland Electric	Yes
Southern California Edison Company	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Northeast Utilities	Yes
Portland General Electric	Yes
MRO NSRF	Yes
NESCOR/NESCO	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
Comment Development SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Utility Services Inc.	Yes

Organization	Yes or No
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes
Luminant	
American Transmission Company, LLC	
Avista	

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
FirstEnergy	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No

Organization	Yes or No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Serivces Corporation	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No

Organization	Yes or No
MidAmerican Energy Company	No
NV Energy	No
Massachusetts Municipal Wholesale Electric Company	No
Detroit Edison Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
Utility Services Inc.	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (NCR01177, JRO00088)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Western Area Power Administration	No

Organization	Yes or No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
ATCO Electric	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Detroit Edison Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No

Organization	Yes or No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Serivces Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
IRC Standards Review Committee	No
PNM Resources	No
Southern Company Services, Inc.	No

Organization	Yes or No
Western Area Power Administration	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Consumers Energy Company	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Utility Services Inc.	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Tri-State G&T - Transmission	No
Xcel Energy	No
Snohomish County PUD	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Liberty Electric Power, LLC	No
Texas Reliability Entity	No
PJM Interconnection	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Lakeland Electric	Yes
Tampa Electric Company	Yes
New York Power Authority	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
California Independent System Operator	Yes

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Progress Energy	No
Tri-State G&T - Transmission	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
The united illuminating Company	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power, LLC	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery	No

Organization	Yes or No
Company LLC	
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

END OF REPORT