NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

Comment Form B
CIP-004 through CIP-007 Questions

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

				1	2	3	4	5	6	7	8	9	10
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

				1	2	3	4	5	6	7	8	9	10
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

				1	2	3	4	5	6	7	8	9	10
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

				1	2	3	4	5	6	7	8	9	10
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	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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
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	

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
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		

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

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

Group/Individual		Commenter	Organization	1	2	3	4	5	6	7	8	9	10
23.	Group	Scott Brame	NCEMC	X				X					

Additional Member	Additional Organization	Region	Segment Selection

1.	Robert Thompson	NCEMC	SERC 1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
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 B8 – CIP-004-5, R1, R2, R3, R4 or R5:

If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4 or R5 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 SDT made significant changes to the requirements, measures, and VSLs associated with Requirement R1, R2 R3, R4 or R5 of CIP-004-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5. For the purposes of the comment summaries and responses for this question, the requirement number references refer to the requirement numbers as listed in draft 2, unless otherwise noted.

General

The applicable systems section has been reviewed and revised to help ensure consistency within CIP-004-5 and with the other CIP standards. This should also make clear that these requirements are not applicable to Low Impact BES Cyber Systems. The SDT has decided not to include the concept of authorized unescorted electronic access. Individuals with authorized electronic access must be trained and have a personnel risk assessment performed as per the requirements. This applies to all personnel including employees, vendors and contractors. For example, the question on a vendor controlled system would require the vendor to meet the requirements as set forth in CIP-004-5.

The SDT has stricken the “attain and retain” language for the training requirement, but has chosen to keep it for the personnel risk assessment requirements. The difference between those words and “acquire and maintain” are negligible.

The SDT does not agree with the suggestion to make Requirements R2 and R3 an expansion of the awareness program instead of training. The SDT believes that for protection of these BES Cyber Systems more targeted training is needed.

The guidelines and technical basis section has been updated to better align with the new draft content and organization. One areas of focus is the training content on networking hardware and software and other issues of electronic interconnectivity. More description around the criminal history check has also been added.

Requirement R1

The SDT has added language in the change rationale section to reinforce the concept that a registered entity does not need to ensure or prove all authorized personnel have received awareness. The language in R1.1 has also been revised to further clarify this point through the use of the word, reinforces. Also, the SDT has added language to clarify that awareness of cyber security practices can include physical security information.

The SDT appreciates the suggestions to allow the registered entity to define the timeline for awareness reinforcement or their own quarters, but believes the language is best retained as written for consistency.

In the measures for Requirement R1, the SDT has removed the reference to “documented security awareness program” and has modified the language to be consistent with the other CIP standards. The language, “not limited to” has also been revised and reviewed for consistency across the standards.

Requirement R2/Requirement R3

These two requirements have been combined into a single requirement which covers the training content in R2.1, in a single table, and the training frequency in R2.2 and R2.3. Another key change in R2 is the modification of the language to clarify that the registered entity is able to determine their training program(s) to fit their needs and it can be based on role, function or responsibility. In concert with this change, Table R2 section 2.1 was deleted to help eliminate the language focusing on role based training. Training is required of individuals with authorized, unescorted physical access or authorized electronic access as per the revised R2.2 and R2.3. In addition to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, the SDT believes training is also needed for individuals with access to Physical Access Control Systems and Electronic Access Control or Monitoring Systems. Also, the SDT has removed the reference to BES Cyber Systems in Table R2 formerly in sections R2.2, R2.3 and R2.4. For Table R2 previous section 2.5, the Change Rationale has been modified to reflect this is a new training requirement. Also, this training should be tracked for personnel involved in the visitor control process in accordance with Table R3 section 3.2 The SDT agrees that recovery plan information referenced in Table R2, previous section 2.8 should be labeled appropriately. The training content on cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets will remain in Table R2 as it is a new requirement from FERC Order 706 and the SDT has provided additional guidance to clarify the intent of this entry.

For Table R2, previous section 2.2, the SDT believes the training should be focused on policy content, not availability, and has made no changes. In Table R2, the SDT has chosen to retain both identification of incidents and response to incidents as separate content as the personnel who need to be trained on each may be different. The scope of training on recovery plans is left to the registered entity and no changes have been made to the standard. Also, the SDT believes the focus of recovery is the specific recovery plans, not the business impact analysis. The measure for Table R2 has been modified to focus on training material as evidence and the guidance has been revised to reflect the type of content this training should include.

The SDT has edited the language formerly in R3 for clarity with removal of the role based reference and the attain/retain language. Since there are no references to evidence retention in the requirement part 1.2, evidence retention, of the compliance section of the standard applies. The reference to documentation that was in Table R3 section 3.1 has been removed as it is covered in the measure.

The SDT does not agree that access to Low Impact Cyber Systems need the training defined in R2. Also, R2 has language included (in a manner that identifies, assesses, and corrects deficiencies) as suggested by some comments to allow detection and correction of flaws. The proposal to allow the registered entity to define the timeline for training was not supported by the SDT. For 2.2 and 2.3 (formerly in Table R3 section 3.2), the SDT believes the language is sufficiently clear that the time interval is between training dates and does not need that language added. BES Cyber Systems was changed to applicable cyber assets in 2.2. The two entries on initial and recurring training are now in Table R2. The SDT has revised the language in the measure for these two entries to make it clear the focus is on training records which should include training date and date access is granted.

Requirement R4/Requirement R5

As suggested, the SDT has combined these two requirements into one and it is now Requirement R3. The SDT has modified the language formerly in Requirement R4 to help clarify that identity confirmation and criminal history check are part of the personnel risk assessment (PRA). The PRA is the outcome of the process or criteria used by a registered entity to evaluate the results of the identity verification (for the initial PRA) and seven year criminal history records check to determine what, if any, authorized access to grant to employees, contractors or vendors. The level of documentation for the process or criteria is left to the registered entity, but should be sufficient for a third party to understand how the decision is made. In defining the seven year criminal history records check, it is not the intent for the registered entity to evaluate the individual's residence locations, education or prior employment. The language has been revised to indicate the criminal history records check should cover locations where the individual has resided/lived for six consecutive months during the past seven years. The initial identity confirmation, even if performed under prior versions of the standards, is sufficient for the employment duration of the individual. The initial identity verification, criminal history check and PRA should be retained in accordance with requirement part 1.2 in the evidence retention component of the compliance section of the standard. A PRA performed under previous versions of the standards is valid until it reaches the end of its seven year lifespan. The intent of the SDT is that the PRA in effect is no older than seven years. The SDT has provided guidance on the acceptable documentation for an exception to the seven year criminal history records check which includes agreements with labor unions. If the registered entity is unable to fully complete the seven year criminal history records check, the SDT feels it is important to document the reasons for the exception so it will not be removing that piece of the requirement. Also, the timeframe for renewal of the criminal history records check is currently seven years and the SDT believes it should remain as such. Drug and alcohol checks are typically performed by entities under an existing program and the SDT chooses not to add this to the requirement. In section 3.3 of the new Table R3, the term process is used to define the method used by a registered entity to evaluate the results of the criminal history records check. Although a "Transportation Worker Identification Credential (TWIC)-like" program would be helpful to facilitate compliance with the PRA requirements, the SDT does not have the authority to make that happen. Measures – The Measures have been revised to focus on examples consisting of documentation. For example, a dated copy of the current PRA, which was performed in the previous seven calendar years, would be sufficient.

VRF/VSL

The language in the VRF for R2 has been changed to remove the reference to role based training. The SDT reviewed the VRFs for R3, R4 and R5 (as indicated above, R3 from draft 2 is now in R2, and R4 and R5 from draft 2 have been combined into R3 in draft 3) to consider if the rating should be a Lower risk factor. The SDT believes the risk associated with violations of these requirements is higher than for R1 and R2; hence the Medium risk factor is appropriate. The VSL for R1 has been modified to include the case where the Responsible Entity failed to implement on-going security awareness for two or more consecutive quarters as the next step above the criteria for High. Since the Medium severity level is for missing two content topics, the High should follow as three or more, not four or more. Commenters also asked whether the size of the company matters in the VSL for R3 (which is now in R2). In response, the SDT has modified the VSL for High and Severe according to the suggestion. The VSL targets the BES Cyber System and does not account for company size. Commenters suggested the Moderate and High VSL language for R4 (now R3) should be swapped on the basis that not performing an identity verification and a background check is worse than failing to document the results. (Also, the incorrect reference in draft 2's R4 to "4.5", which does not exist, has been corrected). In response, the SDT has modified the language for the Severe VSL to include the case where a registered entity failed to implement its PRA processes. Commenters also asked whether the size of the company matters in the VSL for R5 (which is now in R3). In response, the VSL targets the BES Cyber System and does not account for company size.

QUESTION B9 – CIP-004-5, R6 or R7:

If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 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 major concerns with CIP-004 Requirements R6 and R7 center on removal of access privileges under various categories of termination actions. In addition, there were repeated instances noting a lack of clarity regarding access approvals, personnel transfers or reassignments and the proper storage and handling of NERC CIP information.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5.

Applicability Section

As in other Version 5 standards, in CIP-004, requirement part 4.1 (formerly part 6.1), there were several comments on changing instances of Medium Impact BES Cyber Systems to "Medium Impact BES Cyber Systems with External Routable Connectivity." Commenters also commented that "dial-up connectivity" should be removed from the applicability section to be consistent with the applicability sections of other Version 5 standards. In both of these cases, the SDT has revised the standard to reflect these comments.

Requirement R4 (formerly R6) General Comments

Multiple commenters recommended that new or additional items or items currently found in the rationale section should be modified and listed as requirements at the requirement level.

Comments suggested modification to allow for self-correction in certain cases, so that each responsible entity shall implement: measure performance to detect flaws; correct detected flaws expeditiously, and if needed take corrective action to prevent recurrence of flaws. This is a general requirement that applies to the Requirement R4 (formerly R6) sub requirements. Though not necessary from a procedural perspective, more instruction on what needs to be considered in the standards is better than insufficient information. The SDT has incorporated the correcting deficiencies modification to the implementation wording in CIP-004-5 in Requirements R2, R3 and R4.

Commenters recommended that the rationale discussing controls for BES Cyber Systems without user accounts should be added to the appropriate requirements in Requirement R4 (formerly R6). The SDT has moved that discussion from the rationale section to the requirement tables.

A commenter suggested that requirement parts 4.2, and 4.3 (formerly covered in parts 6.2, 6.3 and 6.4) be modified to include requirement parts 4.11, 4.12 and 4.13 (formerly parts 6.11, 6.12 and 6.13) along with part 4.1 (formerly part 6.1) in the requirement table. The SDT has combined requirement parts 4.2, 4.3 and 4.4, which now directly reference those sub-parts in part 4.1.

R4.3 (formerly 6.3)
Commenters recommended that there be a corresponding annual review of provisioned physical security privileges necessary for performing assigned work functions. The SDT has combined requirement parts 4.2, 4.3 and 4.4 (formerly parts 6.2, 6.3 and 6.4). The measures in the new requirement part 4.2 call for signed documents, automated workflow approvals or email showing persons with access have authorizations and similar or the same records showing the consideration of appropriate privileges on the basis of need…" These measures apply to electronic access, unescorted physical access into a PSP and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Part 4.3 (formerly part 6.5)
Commenters asked for clarification on the reviews of authorized and provisioned electronic access and unescorted physical access. The SDT has modified part 4.3 to clarify the requirement. It now reads "verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records."

R4 (formerly R6)
Some commented that the measures for 4.1 (formerly part 6.1) should include unescorted electronic access. The issue with this is that electronic access, by its digital nature cannot be escorted. Consequently, there is no “unescorted” electronic access. Electronic access to data or systems is either authorized or unauthorized. One could call it “supervised” access but the problem lies with a “supervisor” having to be continuously diligent and unerringly able to determine if the supervised user is doing anything malicious. This is not possible and frankly constitutes a threat to network integrity and data confidentiality. The recommended option would be to identify those contractors who require electronic access and run them through the personnel appraisal and the training processes and grant them appropriate access privileges. There are no other means to help ensure there are no unauthorized accesses or data disclosures.

Requirement Part 4.1 (formerly 6.1)
One commented that formerly sub-requirements 6.1.1, 6.1.2 and 6.1.3 (current 4.1.1, 4.1.2 and 4.1.3) would be clearer if the requirement was written, “Designate one or more individual(s) to authorize one or more of the following types of access”. The SDT has changed the requirement to “have a process to authorize”. This negates the need to specifically identify an approver and highlights consideration of “need” for physical access, electronic access and access to “designated” physical and electronic storage locations for BES Cyber System Information.

One commenter suggested that current requirement part 4.1 should include the names and roles of individuals who authorize the various types of access. The SDT has changed the requirement to “have a process to authorize”. This negates the need to specifically identify an approver and highlights consideration of “need” for physical access, electronic access and access to “designated” physical and electronic storage locations for BES Cyber System Information.

One commenter recommended changing the term “designate” in current requirement parts 4.1, 4.2 and 4.3 (formerly parts 6.1, 6.2 and 6.3) to “identify.’ The SDT has changed requirement 4.1 to “have a process to authorize”. This negates the need to specifically designate or identify an approver and highlights consideration of “need” for physical access, electronic access and access to “designated” physical and electronic storage locations for BES Cyber System Information. The SDT has also combined 4.2, 4.3 and 4.4 into a single requirement (4.2).

Several commenters pointed out that access to physical and electronic locations where BES Cyber System Information is stored should have greater clarity around the word “physical”. The requirement part 4.1 (formerly part 6.1) has been changed to clarify storage locations for BES Cyber System Information. It now reads, "access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Several commenters recommended revising the phrase "unescorted physical access" to "unescorted physical access into a PSP." The SDT agrees and has made that change.

Multiple commenters stated that requirement part 4.1 (formerly part 6.1) should allow for roles in the designation of those individuals who can authorize the various accesses. The SDT believes that changing the requirement to "have a process" allows the entity the flexibility to construct their authorization process in a way that best suits their needs.

Requirement Part 4.2 (formerly Part 6.2)
Several commenters recommended that requirement parts 6.2 and 6.3 be revised for clarity. They proposed that requirement parts 6.2 and 6.3 be changed to read, "the individual(s) or role(s) designated in requirement part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." To respond to the comment, requirement parts 4.2, 4.3 and 4.4 have been combined into a single requirement part 4.2. At the same time, the individual authorization has been replaced with a process in requirement part 4.1. The process merely provides a means to authorize, and is implemented in the manner preferred by the Responsible Entity.

Several commenters also suggested that instead of the phrase "deemed necessary," "deemed appropriate" would be more accurate – stating that deeming appropriate is easier than deeming necessary. The SDT used the term "necessary…for performing assigned work functions" to better focus on specific accesses and minimize generalization and audit interpretation issues.

One commenter suggested the phrase "Responsible Entity" be removed from parts 4.2, 4.3 and 4.4 (formerly 6.2, 6.3, and 6.4). The requirements state "that the Responsible Entity determines is necessary." The SDT believes that the term "Responsible Entity" removes a degree of specificity that could be problematic if individuals change frequently or the determination of "necessary" is made by more than one individual within the organization. The SDT has combined requirement parts 4.2, 4.3 and 4.4 and has referenced a process required in part 4.1 "have a process" that allows flexibility to establish authorization frameworks tailored to the Responsible Entity's needs.

One commenter stated that the phrase "need to know" in requirement part 4.2 (formerly Part 6.2) is difficult to quantify and is subject to interpretation. They recommended removing that phrase, believing that approvers who grant all access "deemed necessary" strongly indicates that determinations of need to know are part of the authorization process. The SDT has removed references referring to "need to know."

Many commenters recommended revising the phrase "unescorted physical access" to read "unescorted physical access into a PSP." For clarity, the SDT has changed the wording to "access into the Physical Security Perimeter."

One commenter stated that requirement part 6.3 (now covered under new part 4.1) implies that determination of need for performing work functions is needed for each physical access. They recommended that Responsible Entities document all roles and activities in advance, negating the need for the Responsible Entity restating access they have "determined is necessary." The SDT has combined the requirement parts 4.2, 4.3 and 4.4 and established a requirement for a "process" to develop an authorization framework best suited to the Responsible Entity's needs. This will allow the commenter's company to document all roles and activities in advance if that is the company's preference.

One commenter recommended removal of the phrase "for performing assigned work functions" due to concerns with potential interpretation requests. The SDT believes that since "work functions" are not subject to audits, there is no need to remove the conditional phrase. In addition, there must be some frame of reference for authorizing accesses and work functions are a logical baseline.

Many commenters suggested changing the wording of requirement part 6.4 (now covered under new part 4.1) from "location" to designated repository. The SDT believes that specifying a designated location is less subject to interpretation and in most cases exempts portable equipment from being identified as a "repository" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

One commenter questioned the following: Is the "intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format?" The SDT believes that unescorted physical access includes to both hard copy data and access to equipment used for storing electronic copies. Although physical proximity to equipment does not constitute electronic access, from an information protection standpoint, access to that equipment could result in damage or destruction of those devices storing electronic copies.

One commenter suggested that in requirement part 6.4, (now covered under new part4.1)to eliminate ambiguity, that the term “necessary for performing assigned work functions,” be replaced with “appropriate for the roles and responsibilities.” The SDT understands the concern. In this case replacing “necessary” with “appropriate” does little to eliminate ambiguity. In addition, both terms are likely to prompt interpretations. Also, not all entities are configured to grant authorizations by roles and responsibilities. To address the entirety of the CIP affected population, the SDT believes that the original wording provides more universal applicability.

One commenter believes that requirement part 6.4 (now covered in new part 4.1) should be separated into two requirements. The first requirement would be to identify the repositories that store either physical media containing BES Cyber System Information (paper copy) or the electronic storage of BES Cyber System Information. The second requirement would be the authorization of access to only those designated repositories that have been identified by the entity. The SDT believes that using the term “locations”, as long as they are “designated” serves the same purpose as an identified repository. Because “designated” has been added to the requirement, so must a measure to acknowledge the existence and itemize “designated storage locations.” This will add another measure but will also reduce the potential for audit interpretation and ambiguity.

One commenter recommended that the words “are necessary for performing assigned work functions” be replaced simply with “are necessary”. The SDT believes that this revision, although more economical, could create a situation where the question is asked “necessary for what?” To avoid that possibility “necessary for assigned work functions” is less likely to prompt questions of scope of authorizations.

One commented that the words “physical and” should be removed because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. The SDT notes that if, as suggested by a number of other companies, “designated locations” are used, incidental, non-designated temporary locations of NERC CIP System Information will not be subject to that requirement.

Former Requirement Part 6.3

Former requirement part 6.3 prescribed specific ways to conduct authorizations and referenced individuals designated in former part 6.1. The SDT has instead changed the language in part 4.1 to require the Responsible Entity to "Have a process to authorize . . .", which could certainly include designating one or more individuals, etc., as part of the process, but the requirements do not specifically prescribe the administrative method of achieving the required performance. Thus, former Requirement Part 6.3 no longer exists in the same manner as presented during draft 2.

Several commenters stated that because of potential minor errors or mismatches associated with the required review of authorizations and provisioned individuals, requirement part 4.3 (formerly part 6.5) should be subject to the FFT process. The SDT understands the concern, but FFT is not a function of the requirement. That is a function of potential violations and determined after the fact, not in the standard requirement itself.

One commenter recommended that the following statement from the rationale for requirement part 4.3 (formerly part 6.5) be entered into the requirement or its Measures section: "If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement." While that statement offers some clarification in guidance, the SDT cannot add a requirement or measure that makes a determination whether or not a particular error is a violation.

One commenter stated that requirement parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) are major scope expansions which were not directed by FERC. They further claim that the requirements overlap and are not contributing to a commensurate improvement to security. The SDT believes that reviews such as those in parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) do in fact provide a means to identify indicators of malicious activities, rogue accounts, retained accounts that are no longer authorized, etc. The fact that FERC did not direct the requirement development does not negate the validity or the need for the requirements.

Several commenters recommended adding "currently" between "individuals provisioned". The SDT agrees with the recommendation and will take appropriate action. The SDT has reworded the requirement part 4.3 (formerly part 6.5) to "individuals with an *active* electronic access…"

One commenter stated that requirement part 4.5 (formerly part 6.7) should be revised as follows, “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.” The SDT believes that there must be a specified review period and associated evidence to ensure that Responsible Entities consistently meet the requirement.

One commenter suggested adding the words "to BES Cyber Systems" after the words "physical access" in part 4.3 (formerly part 6.5). The SDT believes this proposed revision is already addressed in the Applicable Systems section of the requirement.

One commenter suggested that in the measures section, there should be consistency of word order between "dated document of verification..." and "documentation of dated verification”. The first measure asks for “dated documentation of verification,” which simply provides a point in time wherein the verifications were performed. The second measure requires a document that provides times of specific verifications themselves, of authorization for access and provisioning of access. The SDT changed the language to provide clarity and consistency to the measure. The consistent language now reads, “dated documentation of the verification.”

Requirement Part 6.4

One commented that the measures in requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) contain contradictory constructions. The background section states that a numbered list includes all required evidence. In the measure, however, these parts state that evidence “may include, but is not limited to.” The SDT has added the phrase “that includes all of the following” to reconcile the format with the intent of the measure.

Several commenters stated that the wording in requirement part 4.4 (formerly part 6.6) is too prescriptive, specifically “verifications that all user accounts, user account groups, or user role categories and their specific associated privileges.” They proposed substituting that wording to read, “verifications that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities.” The SDT believes that the word appropriate is too vague and subject to interpretation. The goal is to verify access to specific accounts. In this case, the existing wording maintains the scope and leaves no ambiguity around which accounts require verification. Regarding the list of measures, the SDT has revised the measure by adding “that includes all of the following” to reconcile the format with the intent of the measures.

Several commenters stated that the measures should only require verification that the entity performed the verification while leaving the results of the verification out of the measure. The SDT believes that requiring verification should specify those items to be verified. Asking for a “listing of all accounts/account groups”, a “description of privileges”, “accounts assigned” and ‘verification that privileges are authorized and appropriate” does not expand scope. Confirming that “verification” was performed would assume that all registered entities would perform the verification on the same lists of required items. If the items are not articulated, there are no assurances that the data would be consistently derived or complete.

One commenter recommended changing the words “performing assigned work functions” to “are appropriate”. The SDT believes that the use of appropriate to define specific standard provisions is too vague and subject to interpretation.

One commenter stated that the scope of requirement part 4.4 (formerly part 6.6) has been expanded above and beyond what has been directed by FERC. The SDT has taken very positive steps to meet the requirements of the FERC directives. In establishing some requirements, the only way to effectively validate that the provisions have been met is to identify the need for specific information that links the requirement to the compliance actions. There may be an increased number of these instances. The important factor is that FERC directives do not limit the detail of the required evidence. The SDT believes that the requirement and measures increase the level of security. Unauthorized, expired or mis-assigned access to BES Cyber Systems represents potential vulnerabilities that could be exploited if not addressed with these administrative requirements.

One commenter also recommended that the wording of the “annual requirement” be worded as follows, “once each calendar year of a period not to exceed 15 calendar months between verifications.” The SDT has changed the requirement to read “once every 15 calendar months to incorporate the additional 3 months of previously discretionary time directly into the requirement.”

One commenter believed that the word “all”, referring to user accounts is too broad. Dominion suggested that the word “applicable” be added after “all” to point to those user accounts, etc that are directly associated with the requirement. The SDT has changed the requirement to read “user accounts on all applicable cyber assets” to maintain the appropriate scope of the requirement.

One commented that requirement parts 6.6 and 6.7 should be revised to allow responsible entities to perform verifications of user accounts, user account groups or user role categories and their specific associated privileges at “a timeframe that the Responsible Entity deems necessary.” NextEra also suggested that this also applies to verifying “access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity are correct…" Although there are a number of companies that would comply with the requirement according to its intent under a self-imposed timeframe, there is no way to ensure that this would be the case. The SDT feels that the annual requirement should remain in place to help ensure consistent compliance actions.

Several commenters recommended changing requirement parts 6.6 and 6.7 to remove "all" referring to reviews of user accounts, user account groups, or user role categories. They recommend replacing "all" with "BES Cyber Systems." The SDT believes that reviews should be performed only on applicable cyber assets. The requirement has been revised as follows: "that user accounts on all applicable cyber assets, user account groups, etc.

Some commenters also commented that "locations" in requirement parts 6.4 and 6.7 should be replaced with designated repositories and include a requirement to list the repositories. The SDT has reworded the requirement to read "designated storage locations for BES Cyber System Information, whether physical or electronic." It has also added a requirement to designate storage locations and a measure to provide a list of designated storage locations. This will remove incidental temporary storage on non-designated devices from the audit process.

Some commenters suggested that the language in the second measure, "A summary description of privileges associated with each group or role", be removed. The SDT believes that understanding the privileges associated with specific roles is a necessary data point for verification that the privileges for specific groups are authorized and appropriate for the work functions performed by those assigned to the groups.

Requirement Part 6.5

Many commenters suggested in some manner to move former parts 6.1, 6.4, 6.7, and 7.3 (now, collectively, parts 4.1, 4.5, and 5.3) into CIP-011. In response, the SDT has revised former parts 6.1 and 6.4 to require a process without specifying how to conduct the authorizations. The SDT notes that CIP-004-5's authorization requirements relate to individuals' access, while CIP-011-1 specifies the information protection requirements.

Some commenters expressed concerns that the measures of requirement part 4.5 (formerly part 6.7) do not need to include the phrase "the minimum necessary for performing assigned work functions." In response, one of the most important aspects of authorizations and privileges is that they be granted using a "least privilege" approach. Otherwise the possibility exists that authorizations are provided or maintained for individuals who do not need them based on expediency rather than a comprehensive review.

One commenter suggested removing the term “minimum” from the third measure of Part 4.5 (formerly part 6.7) since it was removed from the requirement. The SDT agrees with this suggestion and has revised the measure accordingly.

One commenter recommended that the word “privileges” be added to part 4.5 (formerly Part 6.7) after the word “access.” The proposed wording of the requirement would be “verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." The SDT concurs with this addition since it adds clarity to the requirement. It has added “privileges” to the requirement. In a related recommendation, another commenter suggested the word “privileges” be removed from the measure since it is not in the Part 4.5. Adding the word privileges as discussed above will alleviate those concerns.

Some commenters recommended removing requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) because they are too prescriptive in their attempt to accomplish requirement part 4.3 (formerly part 6.5). The SDT believes that verification of requirement part 4.3 hinges upon the existence and validation of requirements listed in 4.4 and 4.5.

One commenter also questioned whether a listing of authorizations is the same as a list of those with access. Authorizations provide a type of eligibility for access. A list of those with access may include someone without that authorization and a potential security issue. That is why the reviews of authorizations, access and privileges are critical to compliance with the standards requirements.

Requirement R5 (Formerly R7) Applicability Section

A few commenters suggested that the applicability of revocation requirements in CIP-004-5 R5 (formerly R7) for interactive remote access should be modified to exclude dial-up connectivity. In response, the dial-up connectivity reference is removed from CIP-004-5 in its entirety.

Commenters also recommended that applicability to “Medium Impact BES Cyber Systems” be limited to those with “External Routable Connectivity” to maintain consistence with other cyber systems/assets currently covered by similar requirements in CIP-004. External Routable Connectivity has already been added to the applicability section for CIP-004.

Requirement R5 (Formerly R7) General Comments

Several commenters expressed concern on requirement part 5.2 (formerly part 7.2) for transfers and reassignments. They believe that the timing of access removal should be based on the determination of when access is no longer necessary, rather than limiting it to a specific time frame related to the transfer or reassignment date. The SDT has revised part 5.2 (formerly part 7.2 as follows: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access".

For requirement part 5.1 (formerly part 7.1), a commenter suggested that part of the FERC Order 706 be more clearly reflected in the requirements. Specifically they would like documentation in the requirement that highlights FERC's statement that exceptions to revocation policy are allowed as long as they are properly documented for audit purposes. Paragraph 462 of Order 706 states that, "revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible." In response, this is not a SDT issue. Creating exceptions for directives in a FERC Order is a separate process undertaken by the ERO. In any event, it is not simply a documentation requirement. Circumstances warranting exceptions have to be identified and then approved. This of course is done against a backdrop of "immediate" revocation stated in the order.

A few recommended that the requirement for revocation based on the "next calendar day" should be changed to "next business day." Another commenter proposed that "next calendar day" be replaced by "within 24 hours." The SDT believes that next business day does not fall under the intent of the FERC Order Directives. Next business day if a weekend or holiday period is in progress could extend the revocation process for two or three additional days. "Within 24 hours" is actually less time than is allowed by the "end of the next calendar day." For the purposes of these comment responses, the SDT feels that next calendar day best meets the FERC Order directive and provides better security than next business day.

Some commenters also expressed concern that the 24 hour revocation requirements may not realistic given numerous and diverse HR and IT processes throughout the industry. Essentially they, along with one other commenter, advocated returning to a framework that allows different time frames for different types of termination actions. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (which may allow for internal processes that serve as trigger points) at the time of the termination action and completing the process within 24 hours, the SDT believes this is a reasonable time frame.

Requirement Part 5.1 (formerly 7.1)

Commenters recommended that the criteria for termination action timeframes should include a reference to the communication of the intention to terminate to provide a type of time stamp for gauging compliance with related requirements of the standard. While the communication of a termination action is not mentioned specifically in the requirement, initiating the process required by requirement part 5.1 (formerly part 7.1) would probably include those trigger points for individual companies. This allows greater flexibility and more concise monitoring of the required timeframe.

Several commenters expressed concern with the format of the measures in Requirements R4 and R5 (formerly Requirements R6 and R7). They are concerned that the background section states that all numbered lists in the measures are all required evidence. However, the measure list states that the "evidence may include but is not limited to." The SDT has revised the measures by adding the following statement: "An example of evidence may include, but is not limited to *documentation of all of the following*: This sentence is followed by numbered measures. This is primarily a formatting issue and this revision should alleviate the discrepancy.

One commenter suggested that the requirement should include "disable or revoke all individualized domain user accounts held by the terminated staff." The SDT believes that removing unescorted physical (preventing any entry into an entity's facilities) and interactive remote access should prevent any further access by the individual after termination.

Some commenters stated that requiring access revocation within 24 hours for all types of terminations is overly burdensome. They believe the 24 hour requirement should be limited to "for cause" terminations with additional flexibility built in for other situations. Other commenters recommended that the 24 hour time frame should apply only to High Impact Assets. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (allowing for internal processes) at the time of the termination action and completing the process within 24 hours, the SDT feels this is a reasonable time frame.

A few commenters stated that requirement parts 5.1 and 5.5 (formerly parts 7.1 and 7.5) seem inconsistent regarding shared user accounts. The SDT sees no inconsistency and believes that the current requirements are clear and sufficiently differentiated. Requirement part 5.1 considers the first tier of access; unescorted physical and interactive remote electronic access. Requirement part 5.5 specifies changing passwords for shared accounts and provides a 30-day time frame for its completion.

One commenter recommended a change to part 5.1 formerly part 7.1) that changes the 24 hour requirement to the end of the next business day after the effective date and time of the termination action. The SDT believes this falls outside of the FERC Directive intent, particularly as it applies to the "next business day." The next business day could increase the access revocation time frame to well over the 24 hours currently stated in the requirement.

One commenter recommended that requirement parts 5.1 and 5.3 (formerly parts 7.1 and 7.3) be revised to include a statement on extenuating circumstances associated with the impact of completion of revocation within 24 hours. FERC has allowed "extenuating operating circumstances" which have a specific application in requirement part 5.5 (formerly part 7.5), due to the complexity and scope of the password change task. Extenuating circumstances outside of that definition are undefined and could be misconstrued as any circumstance that is perceived as an impediment to completion of the requirement. In addition, adding "extenuating circumstances" to these requirements could set a precedent for other requirements, negating the timeliness and effectiveness of underlying security intent.

One commenter suggested clarifying language to the wording of the requirement to make it clear that the 24-hour clock is related to the initiation of the termination process, not the complete termination actions themselves. The SDT has clarified that there must be a process to initiate removal of an individual's ability for access. Initiation of the process must be concurrent with a termination action. Completion of the removal is required within 24 hours of initiating the process.

One commenter believes that termination criteria should vary according to the situation. They would like the tightest timeframes reserved for terminations for cause. The SDT has maintained the 24 hour requirement for termination actions based mainly on the FERC 706 Order requirement that termination be executed immediately.

One commenter commented on a situation where a suspended individual is terminated ten days from the suspension date. While the termination action was initiated in compliance with the requirements of R5 (formerly R7), the effective date of the termination shows up in the records as 10 days prior to the action being initiated. The SDT believes that in these situations, documentation of the suspension along with what a suspension entails regarding any network or system accesses, and a documented company statement verifying the entities suspension procedures and subsequent termination should be sufficient to provide evidence of compliance to an auditor.

Requirement Part 5.2 (formerly 7.2)

Many commenters are concerned about the 24 hour requirement for removal of access for those individuals transferred or reassigned. The SDT understands the issue with access often being required after the transfer for various lengths of time. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement to the following: “For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

One commenter would like reassignments or transfers based on the notification of reassignment or transfer. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement and proposes the following changes: “For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Requirement Part 5.3 (formerly 7.3)

A few commenters requested clarification on physical access to BES Cyber Systems and storage requirement wording in general. The requirement specifies that the access applies to those “designated physical and electronic locations where BES Cyber System Information is stored.” In the requirement the term “designated” has been added. For the measures, evidence includes workflow or sign-off forms verifying access removal to “designated” physical areas or cyber systems. The term designated removes the unintended consequence of BES Cyber System Information temporarily resident on work stations, laptops, flash drives, etc. These areas are consequently not identified as storage “locations.”

Some commenters suggested replacing the words “by the end of the next calendar day” to “within 7 days” or 30 days, respectively in the requirement. The SDT believes that since access removal in requirement part 5.1 (formerly part 7.1) will in many cases, constitute removal of access to BES Cyber System Information, that this requirement should retain its original wording. In addition, in FERC Order 706, Paragraph 386 requires that there be "prompt revocation of access to protected information." Seven or 30 days would not be considered "prompt" by FERC.

One commenter commented that "next calendar day" for removal of access to BES Cyber System Information is too short a time span. The SDT points out that FERC Order 706 dictates prompt removal of access.   The phrase "next business day" for example could mean substantially longer time periods over weekends and some holiday periods.

One commenter recommended the use of the word "repository" over "locations" in the requirement. The word "location" was chosen by the SDT to ensure there was no ambiguity within the requirement. Location is considered a general area, with multiple uses and is not limited to a specific function. A "repository" on the other hand, connotes specific use…for storage of BES Cyber Security Information. The use of location will help avoid any tendency toward requiring exclusivity of purpose and preclude potential violations.

One commenter commented that locations should be changed to designated repositories. The SDT believes that specifying a designated repository is less subject to interpretation and in most cases exempts portable equipment from being identified as a "location" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

Requirement Part 5.4 (formerly 7.4)

Some commenters would like to expand the applicability of requirement part 7.4 to include Medium Impact BES Cyber Systems. The SDT has carefully weighed the applicability of requirement parts throughout the family of Version 5 CIP standards, and, on balance, it believes that the levels of protection for Medium Impact BES Cyber Systems in other requirement parts throughout CIP-004-5 provide an appropriate balance in applying impact-based protections that are graduated between High Impact BES Cyber Systems and Medium Impact Cyber Systems.

One commenter suggested a revision for recovery of all information copied from repositories. The SDT notes that the requirements set out the requirements that must be part of the required processes. The SDT believes that the information protections in CIP-011-1 and the access requirements in CIP-004-5 adequately serve the purpose of protecting BES Cyber Systems while allowing sufficient flexibility to entities in implementing their processes or programs.

A few commenters recommended changing “Requirement parts 5.1 and 5.3 (formerly parts 7.1 and R7.3)” to “Requirement R5, Parts 5.1 and 5.3 (formerly R7 Parts 7.1 and 7.3.”)They also recommended changing the word “removal” to “revoke” for consistency with the requirement. Another commenter also suggested changing “revoke” to either remove or disable. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. The SDT has retained “removal” in part 5.1 along with a clarification which is provided in the requirement language. The SDT retained the term “revoked” in part 5.3 to conform to the overall R5 Requirement.

One commented that the phrase "revoke individual users accounts on BES Cyber Assets" should be changed to "revoke individual access to BES Cyber Assets." The commenter believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for the commenter’s field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays - Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay. It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time.

One comment suggested that in CIP-004 R5.4 (formerly R7.4): “For Termination actions, revoke the individuals user accounts on BES Cyber Assets...” to, for termination actions, revoke the individuals access to BES Cyber Assets...” The SDT has modified part 5.4 to read, “for termination actions, revoke the access to individual’s user accounts (unless already revoked in accordance with requirement parts 5.1 or 5.3) (formerly parts 7.1 and 7.3) within 30 calendar days of the effective date of the termination action."

Some commenters disagreed with the statement that the word "revoke" in this case means to "delete" the user account from the system. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original Globally Unique Identifier (GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GUID will have been lost and difficult to track past account activity. This may be true for other operating systems as well. If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. The SDT has used the term revoke to essentially make an account "inactive". It does not delete the account. Also, requirement part 5.4 has been modified in the "Applicable Systems" section. It now includes only "High Impact BES Cyber Systems and Electronic Access Control or Monitoring Systems that are associated with High Impact BES Cyber Systems." Further, the requirement allows revocation of individual's user accounts within 30 days of the effective date of the termination action.

One commenter questioned that since there is no requirement for revocation of balance of access in 5.4 (formerly part 7.4) for Medium Impact BES Cyber Systems, is there a particular timeline required? The commenter recommended that a timeline be developed that provides auditable records for removing balance of access. In response, the SDT notes that requirement part 5.4 in the applicable systems does not include Medium Impact BES Cyber Systems.   Under those circumstances the audit process would not be considering Medium Impact balance of access.

Requirement Part 7.5

One commenter points out that requirement part 5.5 (formerly part 7.5) only accounts for the 30 days within the requirement and not the 10 days after "extenuating operating circumstances". The SDT has provided measure in part 5.5 to cover that previous omission.

One commenter suggested that the second bullet of the example evidence for requirement part 5.5 (formerly part 7.5) should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. In response, the SDT has modified the measures to clarify that password resets must be completed within 30 days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

One commenter recommended that requirement part 5.5 (formerly part 7.5) be revised to include both terminations and reassignments or transfers. The SDT has added part 5.5 to the requirement to cover the reassignments and transfers.

One commenter suggested that the quarterly review should be converted to a quarterly “cleanup” of individual user accounts and not be considered a violation, and the SDT notes that that a cleanup could certainly a way of identifying, assessing, and correcting any deficiencies, which now modifies “implement” in the main requirement (see summary response to common issues at the beginning of this document), and for that reason, the required performance of the requirement remains a review.

One commented that if an entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it should also apply to allow the Responsible Entity to determine and document that extenuating operating circumstances that can require a longer time period for revocation of access privileges. The SDT believes that since revoking physical and interactive remote (tier 1) access is typically a centralized and relatively uncomplicated process, that the time frames for completion are adequate. In addition, the FERC Order 706 requires “immediate” revocation of access. Providing a conditional caveat “for extenuating operating circumstances would in all probability meet with FERC resistance and result both in subjective application and interpretation.

One commenter questioned the need to modify passwords for shared user accounts if there is no corresponding requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known." The SDT has revised requirement part 5.5 (formerly part 7.5) to accommodate reassignments and transfers as well as termination actions. Requirement part 5.5 reads, “For reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

QUESTION B12 – CIP-005-5, R1:

If you disagree with the changes made in CIP-005-5, Requirement R1 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 SDT made significant changes to CIP-005-5 Requirement R1.

General Comments

One commenter suggested that the communications links between ESP's should be included and that all the External Routable Connectivity exclusions should be eliminated. In response, all BES Cyber Systems have been included within the scope of Version 5 and the blanket exemption filter in CIP-002-5 has been eliminated. The ERC filter is now used on individual requirements where routable connectivity is either needed to meet the intent of the requirement or in general there is insufficient risk from other forms of communication to enforce a mandatory and auditable requirement upon every instance in every registered entity. Communication links have been excluded from this body of standards from the beginning as it is a cyber asset focused standard, and the vast majority of cyber assets used in communications between ESP's are not within the control of the registered entities but are leased services from telecommunication providers.

A few commenters requested clarity around the inclusion of serial devices and another commenter also requested specific clarification concerning the extension of ESPs over large areas via serial communications along with a request for clarification of 'direct serial' used in the guidance. In response, the SDT has focused on the communications requirements of the standards for the highest risk forms of communication – routable protocol networks and public switched telephone network (PSTN) accessible dial-up connections. It is a vital point that all BES Cyber Assets, including all serial devices, are included in the standards and are subject to all the requirements in CIP-003-5 to CIP-011-1 except those where they are specifically excluded. CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication. As to the extension of ESPs over large areas via serial communications, the SDT notes that ESPs are for routable communication only and the SDT does not envision single BES Cyber Systems being defined in such a way that large geographical areas are involved. It is envisioned that a BES Cyber System would encompass cyber assets at a single site only – larger systems would be broken at least into smaller systems by site. For example, a registered entity would not define all the components of an EMS including all field Remote Terminal Units (RTUs) as a single BES Cyber System. The components of that system at each location could be grouped together as the BES Cyber System for that location. Registered entities have great flexibility in their declaration of a BES Cyber System, but need to take into account ESPs and PSPs as well as all other applicable requirements as they do so. In response to the 'direct serial', that is used in the guidance as a term that refers to serial communications that is not routable protocol or dial-up in nature.

One commenter stated that clarity is needed concerning how wireless networks are impacted by CIP-005-5. In response, the SDT notes that these standards are at a higher and logical level and stay above the transport level. The SDT concentrated on protecting the BES Cyber Systems regardless of the physical transport in order to state the goal and also to future-proof the standards against an ever increasing variety of transports. Adequately addressing more detailed technical aspects would require standards per transport. However, the SDT does note that the radio/access point of a wireless network should be considered by the Responsible Entity to see if it should be included as an EAP.

Introduction Section

There was a comment that in the introduction section concerning exemptions (4.2.4) there is a reference to CIP-002-5 that should be CIP-005-5. In response, the SDT has made the change.

Background Section

One comment stated that the applicability of the background section does not address High Impact BES Cyber Systems with External Routable Connectivity and this is used in the standard. In response, the SDT agrees and has added the appropriate language which reads, "**High Impact Protected Cyber Systems with External Routable Connectivity** – Only applies to High Impact Protected Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the Protected Cyber System that cannot be directly accessed through External Routable Connectivity."

One comment read that Medium Impact BES Cyber Systems at Control Centers should be "associated with" instead of "located at". In response, the phrase 'located at' is used to appropriately limit the scope as the case could be made that every Cyber Asset is ultimately ‘associated with’ a control center and could inappropriately identify every Cyber Asset as high impact.

One commenter stated that the section concerning Medium Impact BES Cyber Systems with External Routable Connectivity have the last sentence be deleted as it requires not treating the cyber system as one system, but as individual Cyber Assets. In response, there are several requirements (CIP-007-5 in particular) that do apply at the individual cyber asset level within a system and this sentence clarifies that for those requirements only those cyber assets within a system that have external routable connectivity are in scope if the requirement has this applicability.

Requirement Part 1.1

Many commenters commented that the applicability should include the ERC filter and thus remove the applicability language from the requirement itself and also make it parallel with R1.2, potentially even combining R1.1 and R1.2 into one. In response, the two requirements are purposely not parallel. R1.1 requires an ESP (a ***logical*** border) around every routable protocol network that contains a BES Cyber System even if it is an isolated network and has no external connectivity. The logical border (ESP) is used then as a boundary to define the ‘associated Protected Cyber Assets’ and raise the impact level of the included Cyber Assets to the 'high water mark' of the highest impact level system in the ESP. R1.2 is an additional requirement for those networks that have external routable connectivity to protect that external connectivity. In essence, Requirement R1.1 is the “identify your associated PCA’s and adjust your impact levels” requirement. R1.2 is where external routable connectivity comes in and the logical border becomes more physical with the requirement of Electronic Access Points (EAPs).

Many commenters responded that the applicability needs to be removed from the requirement and the measure. Others commented that Associated Protected Cyber Assets should be included in the applicability as well. In response, the SDT has added the Associated Protected Cyber Assets to the applicable systems column.

There was one comment which stated that documentation on ESP’s on isolated networks provides no reliability benefits. In response, the standards are concerned with all threat vectors, not just those originating from external networks. Portable media and insiders are two of many other threat vectors that can reach isolated networks. The SDT feels that knowing what all other network neighbors are on even isolated routable protocol networks containing a BES Cyber

System (the ‘Associated Protected Cyber Assets’) does have a reliability benefit. The logical border concept of the ESP also defines a ‘trust zone’ where all Cyber Assets sharing a network with a BES Cyber System need to be protected to equal levels, even on isolated networks.

One commenter stated that the measure should allow for documentation at the BES Cyber System level rather than the individual component level. In response, the SDT agrees and has made a change to the measure to allow documentation at either level.

One commenter requested clarification on whether ESPs are required for EACMs and PACMs. In response, the SDT clarifies that ESPs are not required on EACMs and notes that EAPs are EACMs and the standard avoids recursive effect of requiring ESPs around the cyber assets on the ESP. As for PACMs, the SDT notes that without an ability to make a distinction between “field-devices” (i.e. door readers, etc.) and “central servers”, requiring ESPs would be problematic. The intent for protecting PACS is primarily through the CIP-007 requirements for authorization, access control, and logging and monitoring for these systems.

Requirement Part 1.2

One comment stated that the phrase “through the ESP” was redundant in light of the definition of External Routable Connectivity and should be deleted which would also eliminate the use of “through” twice in the existing requirement. In response, the SDT agrees and has deleted the phrase.

One commenter wrote that the measures should include a process to verify that all EAP’s are identified as providing a network diagram is not sufficient. In response, the SDT notes that the requirement does not call for a verification process thus the measure should not imply that is a requirement. The requirement states the desired end goal and the entity is responsible for providing sufficient evidence. Network diagrams that depict all external routable communication paths with identified EAP’s are listed as one possible example.

Several commenters stated that the applicability should be ‘Associated PCA’s with ERC’. In response, the SDT agrees and notes that the PCA for this requirement part are associated with high and medium impact BES Cyber Systems with External Routable Connectivity.

Requirement Part 1.3

A few commenters expressed concerns regarding the monitoring and documentation of all outbound traffic. Inbound only monitoring on PSPs is sufficient and suggest dropping the outbound on ESPs. In response, the SDT believes this is an essential element in combating today's electronic attacks and reiterates the following from the included guidance: "The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked."

Several commenters suggested that the applicability should be "Medium Impact BCS with ERC". In response, the SDT notes that the applicability is to EAPs that are associated with High or Medium Impact BES Cyber Systems specifically. If these applicable systems have no External Routable Connectivity, then they will have no EAPs and the requirement therefore does not apply to those systems.

One commenter suggested that the word "rationale" should be changed to "reason." In response, the SDT agrees as this makes the requirement language the same as that used in the measures and in the change rationale. The change has been made.

One commenter noted that tracking the rationale for 60000 ports is burdensome and asked that this be changed to allow for this on a class basis or ‘criteria’. In response, the SDT notes the requirement does not require that all 65535 ports be documented as this is a ‘deny by default’ requirement and only the remaining open ports (those that ‘grant access’) should be documented. A necessary step in preventing rogue communications to or from a BES Cyber System is to know what the normal communications include and why they are needed.

Requirement Part 1.4

Multiple commenters stated that R1.4 is essentially the same as CIP-007-5 R5.1 and suggest that dial-up be added to CIP-007-5 R5.1 and R1.4 deleted to avoid potential double jeopardy. In response, the SDT notes that CIP-007 R5.1 is specific to user access, while CIP-005-5 R1.4 applies to any access including machine to machine. CIP-005 concerns the security of the ‘network’ level and requires that there be some form of authentication before a ‘network’ connection is established to the BES Cyber System. In essence, there should be some form of EAP-like functionality on dialups. Once a connection is made, then CIP-007 applies as we’ve moved from the ‘network’ level security to device level security and any user access has to be authenticated at the device.

One comment suggested that R1.4 should be deleted as it is included in R2. In response, the SDT notes that this requirement requires some form of authentication for all dialup connectivity regardless of whether it is machine or user based, while R2 only applies to ‘Interactive Remote Access’ which is user-based. The intent of R1.4 is that no BES Cyber System, which by definition can have a 15 minute impact on BES reliability, should be directly reachable by simply dialing a phone number, regardless of how it is intended to be used. Therefore R2 contains requirements that are in addition to R1.4 when the intent of the connection is user based Interactive Remote Access.

Several commenters asked if an entity has no dialup capability to applicable systems, are they required to have processes that would authenticate this access? The commenters suggested that the qualifier ‘if applicable’ be added. In response, the SDT notes the applicability column states that it only applies to systems “with dial-up connectivity” and therefore if an entity has no such systems, there are no systems to which this requirement applies and no process is required. The complete applicability of all requirements throughout the standards is contained within the applicability column and therefore every requirement in the standards has an implied ‘if or where applicable’ clause.

One commenter suggested that the “where technically feasible” clause should be changed to ‘within system capabilities.’ In response, the SDT notes that BES Cyber Systems, which by definition can have a 15 minute impact on BES reliability, should not be directly reachable by simply dialing a phone number. If that is not an inherent capability of the system, then the SDT feels it necessary to add additional equipment with this capability to the system or file for a TFE so that a mitigation plan can be documented to handle the vulnerability.

One commenter suggested that 'where technically feasible' should be deleted. In response, the SDT notes the phrase is an indication of where TFE's may even be requested if the requirement cannot be met on a particular system. Since the SDT is not aware of all situations, it is felt that if an entity cannot meet this requirement on a system that they should be allowed to request a TFE and document a mitigation plan if the TFE is granted.

One commenter suggested that "Associated PCA's" should be added to the applicability. In response, the SDT agrees that any dialup connectivity to any system or Cyber Asset within the ESP, which by definition means the Cyber Asset is also routably connected to a BES Cyber System, should be included. The suggested change has been made.

Multiple commenters suggested that the term 'dial-up connectivity' should be defined to avoid future confusion and should include the notion of access from the PSTN. In response, the SDT is adding a proposed NERC Glossary definition of Dial-up Connectivity.

Requirement Part 1.5

Numerous commenters suggested that the measure only specifies IDS technology and should be made more generic to match the requirement. In response, the SDT agrees and has changed the measure to match the requirement, using IDS as one example.

There were multiple comments that detecting 'malicious' communications requires knowing the sender's intent. Malicious traffic may indeed appear normal. In response, the SDT is adding the phrase "known or suspected" to clarify that the intent is not to detect 100% of all malicious communications, but that communication that has attributes of known or suspected malicious communications.

Multiple commenters asked for clarity as to where the malicious communications inspection should occur and does the direction of the traffic matter. Another commenter stated that only one IDS could be utilized between all ESP's and the

Internet and one per EAP should not be required. In response, the SDT notes the applicability is set at the EAP level and therefore every EAP at Control Centers needs to be covered by the entity's method for detecting malicious communications. The specific architecture and placement is not prescribed. The SDT notes that since this applies to Control Centers, both inbound and outbound traffic should be subject to the detection and has added clarifying language to the standard. For example, if a BES Cyber System in a Control Center begins sending known malicious packets or attempting to communicate with known malicious 'command and control' hosts on the Internet that would warrant detection here and alerting through CIP-007 R4.

Several commenters suggested that the applicability should change to "Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers" as the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks. In response, the SDT notes that the requirement is applicable to EAPs and EAPs are only required where External Routable Connectivity is present, therefore isolated networks would not have EAPs and the requirement would not be applicable. However, isolated networks do have ESPs, so bringing the term ESP into the applicability may further confuse the issue.

There were several comments that raised a concern that the requirement is subjective and may not be feasible for encrypted traffic. In response, the SDT has written this requirement in response to FERC Order 706 and the directive to have two or more security measures at each ESP. The Order further clarifies that this is not simply redundant firewalls, but two separate security measures. The SDT has already reduced the subjectivity somewhat from 'two security measures' to 'detect malicious communications'. In today's technology, this would in most cases (but not all) involve the implementation of an Intrusion Detection System, but the SDT does not want to specify products or toolsets within the CIP standards to help future-proof the requirements. If a better toolset is available in the future that is not called "IDS" we would not want these standards to preclude the use of it, so we've deliberately used admittedly more subjective language ("a method for detecting…") in this case. As to the feasibility with encrypted communications, it is true that the methods will be 'blind' to the content of encrypted sessions but it is left to the entities to determine the relative value between maintaining true end-to-end encryption over terminating the encryption and inspecting the traffic at the ESP. The SDT notes that if the traffic is 'Interactive Remote Access', the encryption must terminate per R2 at the Intermediate Device which cannot reside within the ESP.

In the measures section, there were multiple comments to change the word “and” to “or” and to use bullets. In response, the SDT feels a generic paragraph is easier for clarity than bullets. The measure reads, “Examples of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.”

One commenter suggested that the phrase “where technically feasible” should be added to the requirement. In response, the SDT notes that this requirement is limited to Control Center environments. These are the highest risk locations and the SDT feels that in these instances some form of malicious communications detection (IDS) is always possible on routable protocol communications (EAP’s are required only on routable protocol communications).

One commenter stated that External Routable Connectivity should be added to the applicability. In response, the SDT notes that the applicability is to EAP’s which are only required for routable communication points.

Several commenters stated that detection is only one half of the issue and the standard needs to require addressing or mitigating the detected threat. In response, the SDT notes that EAP’s are EACM’s and are thus covered by CIP-007 R4’s Security Event Monitoring requirements and tie into CIP-008. Therefore the SDT feels that the ‘other half’ of the issue is covered by other standards. Xcel suggests that Intrusion Prevention Systems should be included instead of detection systems. In response, the SDT notes that in a control systems environment, the impact of preventing communications that may be the result of false positives may be greater than allowing the communication. Therefore we do not feel it necessary to require in a mandatory and enforceable manner that all suspected malicious communications should be prevented in all situations. That decision is best made by the Responsible Entity based on the specific situation and potential impacts.

One commenter suggested that the Medium Impact should be removed from the applicability as many of the Cyber Assets can’t perform this requirement. In response, the SDT notes that while many Cyber Assets in substations or plants (field locations) may not be able to perform this requirement, the Medium Impact systems are limited to those in Control Centers where the SDT feels the most risk is present and control center systems typically have the most capability to meet this requirement.

Guidance Section

One commenter stated that the guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP and an apparent conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP. In response, the SDT notes that the Intermediate Device is required only for human-machine interactive login sessions (“Interactive Remote Access”) while the Requirement R1 is concerned with machine to machine sessions as well, which do not require an Intermediate Device. Requirement R2 builds upon Requirement R1.4 when the session meets the definition of Interactive Remote Access.

VRF/VSL Section

There was a comment on how the math is done on the VSL for Requirement R1. The SDT has modified the VSL for R1 to remove percentage calculations. We agree the percentage would be difficult to determine in most implementations. Furthermore, the FERC VSL Order addressing CIP Standards discourages specifying failure to document processes as a lower VSL than failure to implement.

There was a comment that suggested the VSL be medium for high impact and lower for medium impact. In response, the VRF by itself does not account for violations from different types of systems, but the SDT expects the impact level of the BES Cyber System to factor into the assessment of penalties.

One commenter suggested the ROP will need to change with changes to TFEs. Although the SDT does not draft Rules of Procedure changes, the SDT expects that this will be a part of the implementation of Version 5.

One commenter recommended modifying the first “Lower” to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, the commenter recommended moving this VSL to the “Severe” category. The lower VSL is intended for the situation where the entity has only failed to document the process(es). Where the entity has failed to implement one of the technology-based solutions listed in the table, those would fall in the moderate to severe categories based on number of technology-based solutions not implemented. The Lower VSL has been revised to clarify this further. Also by the FERC Guidelines for CIP standards, the failure to document processes should be the same level as the failure to implement a process. We have corrected the VSLs for R2.

One commenter recommended that the VSL for CIP-005-5 R2 VSLs be revised to address the approach to detect flaws; correct detected flaws expeditiously. Upon review of the approach to implement preventive, detective, and corrective controls, CIP-005-5 R2 was not identified as a requirement that would be appropriate for this approach. Therefore, the VSL was not modified as requested.

One commenter agreed that the VRF should be medium for the high impact BES Cyber Systems but that the VRF should be lower for the medium impact BES Cyber Systems. In response, VRFs are assigned for an entire requirement and are not assigned to the underlying sub-requirements or parts.

QUESTION B13 – CIP-005-5, R2:

If you disagree with the changes made in CIP-005-5, Requirement R2 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 SDT has made significant changes to CIP-005-5 Requirement R2. The explanations below describe the changes made based on stakeholder comments – the SDT made other minor edits for improved clarity.

TFE Relevance

In response to concerns that the phrase "where technically feasible" should be removed to eliminate reference of maintaining the TFE process, the SDT notes that TFEs will continue to be used in appropriate requirements unless and until such time that the NERC ROP is modified to address exceptional circumstances. The SDT has reviewed each use of a TFE throughout the CIP Version 5 standards very carefully and specifically, and in each instance where that phrase is used, the SDT understands that there may be circumstances where it could be necessary for an entity.

In response to multiple comments that the applicability of TFEs is not clear within the TFE language included in the overall Requirement language, the SDT has moved the TFE language to the table elements.

Applicability

Several comments stated that instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". This is a valid concern, and in response, the SDT has added the language to the applicability section of the table.

There was also a comment that the requirement should apply to Physical Access Control Systems and systems serving as ESP Access Points. In response, the SDT believes that since these systems generally do not reside within the ESP of a BES Cyber Asset, it would not be appropriate to apply these Requirements to those Cyber Asset types.

Requirement Part 2.1: Intermediate Device

There was a comment requesting that the reference to Intermediate Device be removed from the requirement. In response, the SDT notes that the Intermediate Device is a defined term that is only used within this one requirement. The device functionality is necessary to ensure that proper protections are put in place for Interactive Remote Access sessions. The use of Intermediate Devices allow the client machine to exchange data to a Cyber Asset within an ESP without making direct communication and opening the Cyber Asset to vulnerabilities of the client machine.

Several commenters requested improvements to the language in requirement part 2.1 to clarify that a Cyber Asset cannot initiate Interactive Remote Access. In response, the SDT has clarified the language to address this concern by specifying use of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. However, the language was not modified to address the person using Interactive Remote Access since the requirement is intended to provide protection from malicious software and communications.

Commenters requested clarification on the location of an Intermediate Device and whether an Intermediate Device can also be an EAP. In response, the SDT notes that the definition of Intermediate Device has only one restriction on the location of the Intermediate Device and that is that the Intermediate Device must not reside in an ESP. Other requirements of the Intermediate Device remain flexible to allow the entity to implement a solution that best meets their needs.

Requirement Part 2.2: Encryption

Several commenters requested that the information regarding the purpose of encryption be removed and added to guidance. The use of “in order to protect the confidentiality and integrity of each Interactive Remote Access session” was intended to help clarify the encryption means that were appropriate.This language has been removed, allowing the Responsible Entity the flexibility to implement the level of encryption appropriate to their organization. Additional references regarding encryption are available in the *Guidance for Secure Interactive Remote Access* document. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Several commenters requested clarification on the termination point of required encryption. The requirement states the encryption is to terminate at an Intermediate Device. The Intermediate Device may be one or more assets performing the required functions. Encryption should not be perfromed within the Electronic Security Perimeter due to the negative impact on the monitoring for malicious or suspicous communications.

Requirement Part 2.3: Multi-Factor Authentication

Several commenters requested that the examples of multi-factor authorization be removed from the requirements. In response, the SDT has removed the examples from this requirement part, and the requirement part simply reads, “Require multi-factor authentication for all Interactive Remote Access sessions.”

Several comments recommended more flexibility regarding the use of multi-factor authentication to allow for future technology changes without a Standards update. In response, the SDT has made this change within the measure so that it is listed as an example, but the requirement can account for future technology changes as commenters suggest.

Many comments requested clarification as to where the multi-factor authentication needs to take place. In response, the SDT has modified the Requirement to state that multi-factor authentication to the Intermediate Device is required for all Interactive Remote Access sessions. Furthermore, the definition of Intermediate Device specifies that access control be performed at the Intermediate Device. The Intermediate Device may be one or more assets performing the required functions.

QUESTION B17 – CIP-006-5:

If you disagree with the changes made to CIP-006-5 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 changes to the applicability section, the requirement parts for added clarity, and removal of unnecessary requirement parts that were documentation related.

General
The "identifies, assesses, and corrects deficiencies" language has been added to Requirement R1 and Requirement R2 since these formerly were zero defect requirements. The SDT believes this is an improvement in the compliance process.

The applicability section was renamed to applicable systems to help clarify the scope of that requirement. Also, the applicable systems entries in each table were reviewed to ensure it matched the requirement language for consistency within this standard and with the other CIP Version 5 standards.

The SDT made changes to table R1 to address concerns on the applicability of requirement parts 1.1, 1.2, and 1.3 that had layered versus exclusive applicability. The table no longer uses layered applicability to be consistent with tables in other CIP standards.

The wording of requirement parts 1.2 and 1.3 has been revised to clarify unescorted access is restricted to those authorized for such access, but escorted individuals can enter a Physical Security Perimeter (PSP).

There was consideration of combining monitoring and issuing an alarm/alert into a single table entry, but these are separate actions and needed separate table entries. Even with separate table entries, each is part of a single requirement.

The SDT has removed the 99.9% availability requirement and requirement part 3.2 to document outages for physical access control, logging, and alerting systems. The Physical Security Plan(s) should address how an entity deals with unavailability of these systems.

Requirement parts 1.4 and 1.5 have been modified to remove the reference to circumvention of a control. The new language is monitoring and issuing alarms/alerts for detected access through a physical access point into a PSP. Designation of physical access points to the PSP should be noted in the physical security plan(s).

A PACS is not required to be within a PSP. Unauthorized physical access is to be restricted. The alarm or alert is for detection of unauthorized physical access similar to the language in requirement parts 1.4 and 1.5, although a PSP is not required.

Data retention requirements that differ from the compliance data retention requirements have explicit language in the requirement table. For example, the retention requirement of 90 days for retention of physical access entry logs is specified in requirement part 1.9.

CIP 006 Requirement R1.3

Language has been added to this table, *"… two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters,"* to clarify that two completely independent physical access control systems are not required. For example, a card key and biometric scan using the same Physical Access Control System for validation is acceptable. Also, the SDT has chosen not to use the words "two factor authentication" since, for example, some field locations could use two separate locks. Further, the SDT believes there may be some locations, particularly for field assets, that may not permit two or more different controls, so the TFE clause remains.

CIP 006 Requirement R1.5 & R1.7

The SDT heard the concerns expressed by industry about when the 15-minute clock begins. The language in the standard has been changed to begin once detected. Also, the language referring to the Cyber Security Incident Response Plan remains as that plan could cover physical incidents related to access to cyber assets.

CIP 006 Requirement R1.8

The SDT has chosen to retain the phrase *"… through automated means or by personnel who control entry."* It confirms in the requirement that a person cannot self-log their entry into a Physical Security Perimeter and that the use of a guard is an acceptable method to log entry.

CIP-006 Requirement R2

This requirement does not state that the visitor control program(s) has to be a standalone document/program. If the entity chooses to include the required language within the Physical Security Plan, that is acceptable.

CIP 006 Requirement R2.1

The language in the parenthetical "*(individuals who are known or guests, and not authorized for unescorted physical access)*" has been removed. A "visitor" is anyone who does not have authorized unescorted physical access inside the PSP. This could include employees, contractors, service vendors, etc. The measure indicates that evidence may include documentation of the visitor control program and visitor logs. There is no reference to "proof" that a visitor was continuously escorted.

CIP-006 Requirement R2.2

The language was edited to correct the implication that a visitor exits to a PSP. Also, the measure was modified to better match with the requirement.

CIP-006 Requirement R3

The SDT considered the suggestion to remove the term "hardware" from the phrase "… locally mounted hardware and devices…" used throughout this requirement. This same phrase has been used in previous versions and is understood to exclude hardware such as door hinges, screws, etc. Also, there is new language in the background section regarding applicable systems that provides additional information on locally mounted hardware or devices.

CIP-006 Requirement R3.1

The SDT believes the key role played by the PACS and associated hardware and devices in protecting High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity warrants a 24-month testing cycle. PACS used for Medium Impact BES Cyber Systems without External Routable Connectivity do not have this requirement.

QUESTION B23 – CIP-007-5, R1, R2, R3 or R4:

If you disagree with the changes made in CIP-007-5, Requirement R1, R2, R3 or R4 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,

General Comments

One entity commented that there is a reference in the 4.2.4 exemptions section that refers to CIP-002 but should refer to CIP-007. In response, the SDT agrees and has made the change.

Several commenters commented that either all VSLs or VSLs for certain requirements should be based on percentage of cyber assets missed. Using percentages based on Cyber Assets on CIP-007-5 Requirements is problematic because Requirements do not have a singular mapping to assets. Also, it is possible for a single Cyber Asset to have multiple violations.

One commented that all Severe VSLs should state the phrase “failed to implement one or more documented.” The SDT reviewed this suggestion, and “did not implement” as the SDT proposes is consistent with the SDT’s intent.

Requirement R1 General Comments

One commenter suggested that the rationale section for Requirement R1 needs to include physical ports. In response, the SDT agrees and has added this to the rationale.

Several commenters stated that throughout Requirement R1, the applicability for Medium impact should be limited to Medium Impact with external routable connectivity (ERC). In response, the SDT notes that Requirement R1.1 which applies to network accessible ports is already limited to those systems with ERC. Requirement R1.2 refers to physical ports that could be used by someone physically present to inadvertently or intentionally compromise a BES Cyber System. In this case, ERC does not matter and the SDT believes the ERC exclusion should not be considered in this case.

There were a few suggestions that the High Impact systems should include the ERC filter as well. In response, the SDT notes that since Version 1 of the CIP-002 standard, lack of external routable (or dial-up) connectivity has been a blanket exemption everywhere except Control Centers, where even standalone networks were still to be considered as Critical Cyber Assets. Since High Impact in Version 5 refers to Control Centers, the SDT cannot 'go backwards' without sufficient justification, which we believe is absent.

One commenter suggested that the words "and Services" should be dropped from the title as the requirement concerns only network ports. In response, the SDT notes that ports are opened by services and that typically a port is disabled or closed by disabling the corresponding service. The requirement also allows for services that use wide ranges of dynamic ports that need to be enabled to be documented as the service name rather than a dynamic port range. Therefore the SDT believes the 'and Services' is appropriate.

Several commenters stated that the Requirement R1 measures may also include rationale as to why ports are necessary or clarify in the requirement. In response the SDT agrees and has added a specific measure for documentation of the need for all enabled ports.

Requirement Part 1.1

One commenter suggested that the phrase "ports or services" should be "ports and services". In response, the SDT notes that the use of the word "or" is intentional to allow for circumstances where a Cyber Asset uses one service that is on one port, another service that uses a range of ports, or a service that uses dynamic ports without a defined range (e.g. may use anything over 1024). The entity should be allowed to document the enabled single ports, port ranges, or in the case of the dynamic ports, the service that is enabled. Therefore the SDT feels the word "or" is appropriate.

Two commenters suggested that the sentence in the guidance concerning cyber assets that allow for no port management and therefore all open ports are deemed 'needed' should be part of the requirement. In response, the SDT agrees and has moved the sentence to the requirement.

One commenter suggested that the phrase 'where technically feasible' should be replaced with 'within device capabilities'. In response, the SDT notes that devices that do not allow for port management will have their ports determined as 'needed' thus the TFE will be seldom used. However, the SDT wanted to allow for entities to request a TFE for any special cases.

One commenter suggested that the requirement should consider more than listening ports but should also include unexpected connected ports making outbound connections. In response, the SDT notes that this risk is covered at one level by CIP-005's new outbound rule requirement. The SDT also notes that this requirement requires evidence of a known port configuration for the cyber asset and it is unclear how an entity could perform this for 'unexpected' ports.

Several commenters asked for clarification as to how "associated PCA's" applies and is not an independent set of individual assets. In response, the SDT notes that most of CIP-007, and Requirement R1 in particular, must be implemented at an individual cyber asset level and the requirement thus starts with 'For applicable Cyber Assets'. Ports and services are enabled or disabled on individual Cyber Assets and most of CIP-007 can't be done at a 'system' level but at a Cyber Asset level. For example, if an entity does not need telnet service, then the only way to prove that it has been disabled is on an individual Cyber Asset basis – ports and services are by nature not implemented on a 'group' of Cyber Assets but on individual Cyber Assets.

FMPA and LCEC commented that the SDT should add the phrase "that initiate or receive network communications" after the word "services" or delete services and let ports handle it. In response, the SDT notes that the services is part of "port ranges or services" and are two levels at which the entity can document the enabled logical network accessible ports. This was added primarily to handle dynamic ports. Some systems will use a particular dynamic port out of a small range of ports and documenting that range is acceptable. Other services may pick a dynamic port out of all the high ports (any port between 1024 and 65535 e.g. RPC) and the SDT's intent is to allow for documenting the need at the service name level.

Some commenters suggested that clarification that the Responsible Entity determines the need of port should be included. In response, the SDT agrees and has added clarifying language.

One commenter suggested that the phrase "enable only logical network accessible ports needed" should be "enable only required logical network accessible ports." In response, the SDT notes that the intent is to document the business or technical justification for all open ports. In previous drafts, numerous comments were received to change the word "justification" to "need", which was accepted by the SDT. The SDT also notes there is a difference in "required" and "needed" and thinks "needed" is a more appropriate term due to instances where a Cyber Asset may be fully able to perform its basic function without the port enabled (thus the port is not technically "required"), but the port is "needed" for other purposes. Similarly, KCPL commented that the "needed" should be changed to "approved" for clarity. In response, the SDT notes that these ports are part of the tracked baseline configuration in CIP-010 and approvals occur there. The SDT has therefore not brought in the approval process into CIP-007.

One commenter suggested commented that 'listening' should be replaced with 'enabled'. In response, the SDT believes the term 'listening' is more descriptive as the intended scope is those ports that can actually be reached from the network. A port can be 'enabled' at one level (a config file), but blocked by other means lower in the OS (e.g. TCP_Wrappers) such that it is not actually 'listening'. The end goal is blocking accessibility from the network to unneeded ports and the SDT believes 'listening' better captures that goal.

One commenter suggested that a fourth bullet should be added to the measures to address CIP-005-4 R2.2: Listing of access points to the ESPs, including configuration of ports and services, individually or by specified grouping. In response, the SDT agrees that EAP's should be highlighted and has added this to the first bullet point.

One commenter suggested that the measure should add the phrase "or class of Cyber assets" to the second bullet. In response, the SDT agrees and has added the phrase "individually or by group" to the bullet point.

One commenter suggested that the first bullet under the measures should be deleted as it doesn't meet the requirement. In response, the SDT agrees that a simple listing of port need is not sufficient to meet the requirement and has replaced that measure with the phrase "Documentation of the need for all enabled ports individually or by group".

One commenter suggested that the list of listening ports could be a source of double jeopardy with CIP-010's baseline configuration requirements. In response, the SDT notes that the requirement is concerned only with the enabling of only needed ports irrespective of any documentation. The list of enabled ports is a requirement in the baseline configuration requirement in CIP-010. The SDT believes that failing to maintain the baseline configuration and failing to actually go to a Cyber Asset and disable unneeded ports are two different requirement violations. The measures for this requirement refer to listings of ports as evidence, but that evidence could be the same evidence required for CIP-010. Being able to utilize a single piece of evidence for proof of compliance with two different requirements is not double jeopardy.

There was a commenter who suggested that instead of the phrase 'class of cyber asset' the language from CIP-010 should be used. Also, the requirements should address justification of enabled ports. In response, the SDT agrees and notes that justification is addressed by the phrase 'needed by the Responsible Entity' and the measure has been changed to now call for documentation of the need for all enabled ports. The SDT also agrees with the ‘class of cyber asset’ comment and has incorporated the language ‘individually or by group’ from CIP-010 as suggested.

One commenter suggested that the reference to CIP-005-5 R1 to protect the network in the guidance should be deleted. In response, the SDT agrees and has deleted the language, leaving only the clarification that blocking ports at the ESP does not substitute for the device level requirement.

One commenter suggested that the guidance should allow for disabling ports ‘inline in a non-bypassable manner’. In response, the SDT agreed with this in the draft 1 comment phase and made that change between drafts 1 and 2.

Requirement Part 1.2

There was a comment that the text should be revised to begin with the phrase “Have methods to protect against...” since the VSL is for not having methods. In response, the SDT notes that the overall Requirement R1 is to “implement documented processes” and changing this to have methods would add another level of abstraction such that the overall requirement would be “implement documented processes to have methods to protect.”

A commenter suggested that this requirement should be replaced with a ‘implement a policy’ type requirement. In response, the SDT does not believe that a policy only requirement would meet the FERC directive in Docket No. RD10-3-000 of March 18, 2010, which is the genesis of this requirement.

Several commenters suggested that signage is a weak control that does not provide adequate protection. In response, the SDT notes that signage was never meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. The industry has made several comments as to the other preventative and detective measures that are required before physical access to a physical port is ever achieved. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who plugs his infected smart phone into an operator console USB port “just to charge the battery”.

Several commenters stated that this requirement needs further justification for its existence. In response, the SDT notes that this requirement was added to address FERC's Docket No. RD10-3-000 of March 18, 2010 which states, "However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP reliability standards in general, adequately address technical opportunities to mitigate risks associated with unused physical ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current reliability standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP reliability standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

One commenter stated that entities may not be able to block physical ports based on usage using the example of unplugging a USB keyboard or mouse and using a thumb drive in that enabled port. In response, the SDT notes the requirement is to "protect against the use" and purposefully does not use the verb "prevent" in recognition that the control is not effective in prevention in many cases as the industry has pointed out. The intent of the requirement is not to be a 100% preventative control, but is a last measure in a defense in depth layered control environment to make personnel think before attaching to a BES Cyber System in the highest risk areas.

There was a comment that this requirement should be limited to network ports as portable media is handled elsewhere. In response, the SDT notes that BES Cyber System Information on portable media is handled elsewhere, not the portable media itself. Portable media is becoming a primary means of entry into entities and the SDT believes that to meet FERC's intent, portable media and console command ports should remain in scope.

One commeneter asked for clarity on whether the disabling of physical ports could potentially reclassify a device that would otherwise be considered a BES Cyber System. For instance, if a routable device had all of its physical network ports blocked then what otherwise might be a routable device cannot route. In response, the SDT notes that the ability to communicate outside of itself is not a determining factor as to whether a Cyber Asset is or is not a BES Cyber Asset or BES Cyber System; the Cyber Asset's function as it pertains to BES reliability determines that. So although a Cyber Asset may indeed be a BES Cyber Asset, if all communication ports are disabled then the BES Cyber Asset would have no External Routable Connectivity or dial-up connectivity and thus none of the requirements which have that condition in the applicability column would apply. The specific example of the programmable television monitor provided would have to be determined by the Responsible Entity as to whether the monitor met the definition of a BES Cyber Asset. If the monitor is not a BES Cyber Asset, then it is not a part of a BES Cyber System. The SDT notes that BES Cyber Systems consist of one or more BES Cyber Assets, not every programmable electronic device.

There was a comment asking for clarity as to whether ports could be protected via a common method or must the protections be per port. In response, the SDT notes that the requirement is not prescriptive in this manner and does not preclude either as the measures and guidance allow for directive measures.

One commenter stated that the word “unnecessary” should be changed to “not required”. In response, the SDT is allowing for slightly more flexibility than is denoted by terms such as “required” or “not required”. A port may be “necessary” for some use of the entity but not technically “required” for the operation of the device.

Requirement R2 General Comments

Several respondents commented that patch management should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while managing patches on all Cyber Assets is a best practice, making this a mandatory and auditable requirement would divert the industry’s attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don’t maintain that balance. The SDT also believes that many devices will probably have some portion of the population declared as medium impact and thus many entities will need to handle any vulnerabilities on those devices and oftentimes will just patch all devices of that type.

There were many commenters that suggested that all sub requirements should have the applicability changed to medium impact with ERC. In response, the SDT notes that managing security patches or otherwise mitigating the vulnerabilities the patches address is a core activity in protecting our critical infrastructure. While external routable connectivity does increase the risk, the lack thereof does not reduce it to an acceptable level as many threats enter the environment by other means such as thumb drives, laptops, smart phones, etc. The SDT does not believe we can adequately protect the infrastructure if we only concern ourselves with patching devices with external connectivity due to the remaining threat vectors. However, the SDT does understand the evidence burden and has made changes to this requirement to reduce that burden. The requirement now allows entities to focus on a monthly ‘batch’ cycle of patches rather than tracking timelines for every individual patch, and no documented mitigation plans are needed if patches are installed within the 70 day time period. It is the SDT’s intent that these and other changes in this requirement will relieve the documentation burden while still requiring the performance of this basic security activity. The essence of this requirement is to have the industry watching and aware of vulnerabilities in their BES Cyber Systems, whether they are routably connected or not, and mitigating those vulnerabilities. Many patches may address vulnerabilities that the entity has already mitigated through existing means and require no action. In fact, it is expected that the lack of external routable connectivity would be used as a major factor in many applicability decisions and/or mitigation plans where that is the case.

Several commenters stated that the requirement should not require a documented remediation plan for every patch, but outline a standard patch mgt process with documented deviations. In response, the SDT agrees and has modified part 2.3 to allow for this.

There were a couple of comments that clarification is needed on failed patches installed well after the 60 days but according to the entity’s plan. In response, the SDT has modified the requirements such that a plan may be revised (see requirement part 2.4).

One commenter suggested that the word “processes” should be changed to “program” throughout R2 so it aligns with 2.1. In response, the SDT agrees the terms should match, but notes that Requirement R2 (above the tables) uses the word “processes” and has changed the term “program” in 2.1 to “process” so that the entire requirement uses the same term.

One commenter stated that the requirement in essence rewards obsolescence and never requires upgrading to a patchable system. In response, the SDT notes that the standard’s intent is to secure the infrastructure that is in place without requiring equipment upgrades of currently functional equipment solely for security purposes. Cyber security risks are one factor in the decision to upgrade. The SDT also notes that cyber risk is determined by many factors, and older equipment could actually have a lower cyber security risk. These decisions are best left to the Responsible Entity to make based on the specific circumstances rather than mandated unilaterally in a cyber security standard.

There was a comment that clarity should be provided on what constitutes a “security patch” and what is “updateable”. In response, the SDT agrees and has added clarifying sentences to the guidance section of the standard for part 2.1.

Requirement Part 2.1
Multiple comments stated that the phrase “security patches” should be changed to “patches and security upgrades”. In response, the SDT is concerned with expanding the scope beyond patches to words such as upgrades or updates. The

SDT does not desire to create the situation where a vendor creates a new version of their software, mentions something new about security in the new version, and suddenly everyone is under mandatory compliance obligation to either upgrade or create a plan. Cyber security features are one component of an upgrade decision. The SDT believes that keeping this requirement to the word “patches”, which are fixes to their existing version, is what should be mandatory. The SDT also notes that patches are a fix to a specific vulnerability, which is what the requirement is based upon as it is under obligation to mitigate the vulnerability.

One commenter suggested that applicability and compensating measures should be determined based on original source of patch (e.g. Microsoft) rather than the SCADA vendor. In response, the SDT agrees that this is a best practice so that vulnerabilities may be mitigated in the shortest timeframe possible, even before the patch is certified by the SCADA vendor. The SDT notes that the provided example is the most obvious one with Microsoft, however if included in a mandatory and auditable environment this would extend to the seemingly unlimited non-obvious situations where an entity buys a system from vendor ‘X’, but vendor ‘X’ is using software components from 20 other vendors. The entity does not know all the original sources of all components of the system. Situations such as what is the RTOS (Real Time Operating System) involved in a particular digital relay would arise, and why didn’t the entity track the vulnerability info for that RTOS directly from that vendor rather than the relay vendor’s firmware levels? The entity is not a direct customer of that RTOS vendor and may not have access to that information. In summary, while the SDT believes this is a best practice in some situations, making it mandatory and auditable in every situation is not something that entities can comply with as the standard expands in scope to every BES Cyber Asset in the field.

There was a recommendation that more guidance is needed on appropriate patch sources. In response, the SDT notes that the ‘appropriate sources’ was added to this requirement from Version 4 so that a definite start date for the evaluation timeframe could be determined. The appropriate source is going to be dependent on the situation. If the Responsible Entity has a control system from vendor who invalidates support contracts if the system is patched outside of their approval, then the vendor should be the appropriate source. If the system were custom built by the Responsible Entity, then the vendor for each of the components used to build the system would be the appropriate source.

One commenter recommended that the program should be specified in Requirement R2 and not Requirement R2.1 as a process does not include a program. In response, the SDT agrees and has changed the word “program” in R2.1 to “process” so that it agrees with Requirement R2.

Some commenters said that the process should include a periodic review (monthly) of all patch sources rather than maintaining timeframes per patch. In response, the SDT agrees and has made changes to the language to incorporate this concept.

There was a comment that the requirement should insure that documentation of sources is a onetime exercise unless new software is added to the baseline. In response, the SDT agrees and has clarified this in the guidance section of the standard.

Requirement Part 2.2

Numerous commenters suggested a change to 35 calendar days to allow for a monthly cycle. In response, the SDT agrees and has made the suggested change.

One commenter requested that the guideline states that entities are allowed to evaluate and accept risk which FERC Order 706 disallows. In response, the SDT agrees and has modified the guidance.

There were a few commenters that requested additional clarity on what the term 'applicability' means. In response, the SDT agrees and has added clarification to the guidance section.

One commenter suggested alternative wording, "Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in requirement part 2.1. The assessment must include determination of the applicability of each patch to the entity's specific environment and systems as well as reason for a patch's non-applicability." In response, the SDT has modified this requirement to incorporate a monthly review of the patch sources, but has chosen not to get more prescriptive with the term applicability within the requirement. The SDT believes that evaluating applicability necessarily means that the entity will be documenting the final determination for their environment.

Requirement Part 2.3

Some commenters proposed changes to the timeframe and process such that it would allow 60 days and have no remediation plan required if the patch is installed within 60 days. In response, the SDT agrees and has modified the requirement so that applying the patch or creating or revising a mitigation plan are all choices the entity can take within the second 35 day period. The SDT notes, however, that the timeframe is 70 days total with 35 days for tracking and determining applicability and 35 days for either installing or determining the mitigation plan. It is not 35 days plus an additional 60 days for the second step.

There were multiple comments that the word “dated” should be revised since it is open-ended. In response the SDT believes the word “dated” is necessary and the requirement would be open-ended if it had no date required for the plan. The date of the plan in requirement part 2.3 is what part 2.4 depends upon.

One commenter stated that the requirement was overly burdensome due to the sheer number of patches. In response, the SDT notes that due to the burden the auditable cyber assets are limited to High and Medium Impact Systems and associated systems. The SDT has changed the requirement so that the tracking can be on a monthly basis for all patches released that month rather than on an individual patch basis, which should help.

Some commenters suggested that specificity is needed as to a maximum timeframe. It is compliant with the requirement to state a timeframe of the phrase “End of Life Upgrade”. In response, the SDT has had numerous discussions around this issue. The SDT has decided that the reliability risk of putting prescriptive and mandatory timeframes for patching outweigh the risks of having an open-ended patching timeframe. There are numerous reasons. One reason is the industry goes through periods of time during seasons of the year that we refer to as “nobody is touching nothing” mode because the risk of any change to equipment or systems invokes an availability risk when the asset is depended upon the most. Tripping a generating unit on a 100-degree day because a standard said we were out of time to patch it to fix some minor issue is not acceptable. Another reason is we are in a largely legacy equipment environment as this standard expands outside of control centers where there are no patch management solutions. Upgrading the firmware in thousands of digital relays is something that must be planned and executed very cautiously. Firmware based devices will require planned outages for patches and present the risk of “bricking” the asset. So for these and other reasons, the SDT has decided the implementation timeframe is best left up to the entity rather than enforcing some arbitrary timeframe. The requirement is that they have a dated plan and must work towards that plan. We believe this is the best tradeoff between the risk of someone exploiting a vulnerability and the inherent risk of changing code in devices where availability is paramount. If the SDT set a maximum timeframe to handle these sorts of cases, we would have numerous comments about how the timeframe is too long. We believe that setting a timeframe to handle these cases would actually draw a line in the sand that would have the unintended consequence of all patch timeframes moving toward that timeframe. If the entity has to set its own timeframe and defend it, then they won’t all tend to move towards the maximum timeframe specified in the requirement.

Two commenters suggested that the requirement should allow for revision to an existing plan. In response, the SDT agrees and has changed the language to allow for revisions.

There were a few recommendations that the word “exposed” should be “addressed”. In response, the SDT agrees and has made the change.

There was a comment that a potential double jeopardy issue exists between requirement parts 2.2 and 2.3. In response, the SDT has made numerous changes to these requirements and believes that any double jeopardy issues have been addressed.

One commenter stated that an evaluation of the language in the change rationale should be done to determine what needs to move into the requirement itself. In response, the SDT believes that what remains in the rationale is rationale and has no actionable requirements that could be moved to the requirement itself. However the SDT agrees the language in the rationale should be preserved and has moved it to the guidance section as well.

There was a comment that addressing the vulnerability could be entirely dependent on vendor’s patch development timeframe to address a vulnerability. In response, the SDT notes that the process begins upon the release of the patch from the source identified by the Responsible Entity. The patch has been developed and is available before the process required in R2.2 and following starts.

One commenter asked about the need for TFEs where patches cannot be applied. In response, the SDT notes the intent is that TFEs are not required at any step in the process. The process has been designed to alleviate the need and guidance has been included as well to address this issue.

There was a comment that the first sentence in the guidelines for Requirement R2.3 is a restatement with different wording and may imply other requirements. In response, the SDT agrees and has changed the guidance to more closely match the requirement.

Requirement Part 2.4

Multiple commenters stated that the plans should allow for revision in other than CIP Exceptional Circumstances before the timeframe expires. In response, the SDT agrees and has added the ability to revise the plan if done through an approved process such that the revision or extension is approved by the CIP Senior Manager or delegate.

An issue was raised that there is a potential double jeopardy issue as 2.4 duplicates Requirement R2 where 'implement' is required. In response, the SDT does not believe that a double jeopardy issue exists because the implement in the overall requirement is for the patch management process, whereas the implement in R2.4 is for the individual patch. If R2.4 does not have an implement requirement at the patch level, then the 'implement' in the overall requirement only applies to drafting a plan.

One commenter suggested that guidance should be offered on how much information is expected to demonstrate implementation. In response, the SDT notes that example measures are provided and that the requirement is for the implementation of a mitigation plan, thus the measures would be records of the implementation of the plan. The plan may include such things as installing the patch and the measure would be a record of the installation, or the plan may include the disabling of an affected service, or the adding of a signature to an IDS, or a change to a host based firewall to handle the vulnerability and the measure would be the record of the completion of these changes.

There was a comment that the change rationale is from 2.2 and doesn't address 2.4. In response, the SDT agrees and has updated the rationale to match the changes in the requirement.

To address the comments that bullet 2 of the measure should read "records of vendor recommended or other appropriate mitigations" the SDT agrees and has added "or other appropriate" to the measure.

Requirement R2 VSL

One commented that the R2 and R3 VSLs increment by different ranges. In response, R3 has been modified to remove specific timeframes in the Requirement and the VSL has removed the referenced increments.

Requirement R3 General Comments

One commenter requested that the requirement should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while this is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don’t maintain that balance. The SDT believes that keeping the requirements on Low impact systems at a programmatic level rather than a device level is the only way to keep that balance.

Multiple commenters suggested that the applicability should change to all medium impact with ERC. In response, the SDT disagrees because the threat of malicious code is not limited to introduction through external routable connectivity. The threat of malicious code is arguably higher from portable media, temporarily connected cyber assets (vendor laptops, etc) and inadvertent insider actions.

Requirement Part 3.1

There were a few comments which stated that the intent should be clarified and suggested language includes "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." In response, the SDT notes that the applicability is at the ‘system’ level and the intent is to keep it at that level as this is a requirement where the ‘system’ level is beneficial. Therefore, the SDT believes it is best to not fill the requirement with language at an individual cyber asset level.

There were several concerns that Requirements R3.1 and R3.2 are too vague. In response, the SDT notes that the requirements are indeed written at a very high level but the SDT believes it is necessarily so. Malicious code protection is at the ‘forefront of the fight’ and is rapidly evolving and changing to match the ever changing and morphing threat. The SDT believes the protection of our infrastructure can be better accomplished if we do not have prescriptive technical methods detailed in this requirement. This could have the unintended effect in the future of stifling innovation and the use of new and better tools that would provide better protection but not be compliant with what the SDT would specify today. It does not produce a standard that is future-proof. All previous versions of the standard did prescribe a particular technology and method that must be used on all applicable cyber assets, and while that had no vagueness it became a huge burden on the industry for TFE’s, putting the industry’s focus on what could not be done rather than what could be done. Therefore, the SDT is leaving this requirement at a very high level that is in essence “think through the problem of malicious code introduction, detection, and prevention and come up with the best methods to handle the problem in each particular situation, and then document and do those methods.” The SDT believes reliability will be better served in the long run by a requirement like this for such areas as the malicious code ‘arms race’ environment that we find ourselves in.

There were multiple comments asking if the ‘or’ is appropriate. There was another question if an awareness campaign to deter is ok. There was a suggested that the word ‘deter’ should be stricken. In response, the SDT notes that the requirement was worded with the ‘or’ and ‘deter’ to avoid zero-defect language. If the requirement was to detect or prevent all malicious code, then despite an entity’s best efforts if some zero-day malware did make it onto an applicable cyber asset the entity would be in violation of the requirement. As malware detection and prevention is an inexact science and essentially an ‘arms race’, the SDT did not want to word the requirement in such a way that it required perfection in an imperfect environment with imperfect tools.

There was many comments that the ‘Associated PCAs’ are included at a Cyber Asset (device) level, not a system level and should be deleted or clarified how the ‘system’ concept will apply. In response, the SDT notes that malware prevention really is at a Cyber Asset level and recognizes that the associated PCA’s could be included by reference in the documentation the entity supplies for Requirement R3.1.

One commented stated Requirement R3.1 and R3.2 should be revised to “deploy methods … within an ESP” to scope to routable assets within the ESP. In response, the SDT notes that ESP’s are only required around routable protocol connected cyber assets, however malware protection is required on all cyber assets in scope. Malware is a risk even on isolated systems; it may not be able to easily spread in non-routable environments, but it can be coded to have a specific impact even on isolated systems (e.g. Stuxnet was coded to do its harm when it reached a specific system and could travel by USB portable media). Therefore the SDT has chosen to not limit the malware prevention requirement to only routable protocol accessible systems in ESPs.

One commenter suggested that the measures should be revised to, “Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.).” In response, the SDT notes the only suggested change is the phrase ‘non-software’ in front of ‘policies’. The SDT does not wish to make the measure more prescriptive than the requirement itself. Since malware prevention is an ever changing ‘arms race’ type environment where the controls needed are changing as the threat constantly evolves, the SDT is leaving this requirement at a high level. This will allow entities to adapt as the threat adapts while also reducing the need for TFEs.

One commenter stated that the last sentence of the guidance says ‘should not require a TFE’ making it unclear whether TFEs are an option or not. In response, the SDT agrees and has struck the phrase.

Requirement Part 3.2

One commenter recommended that the following sentence be added: “Mitigation for the Associated Protected Assets may be accomplished through other applicable systems.” In response, the SDT agrees that this is possible and the entity could state how the mitigation covers the associated PCA’s in their documentation for this requirement.

One commenter suggested that the wording “within 35 days” should be added as malware mitigation timeframe. In response, the SDT has chosen not to include a mitigation timeframe as in some cases the entity may be working with government or law enforcement in an ongoing investigation. In APT cases, quick mitigation may just force the moving of the attack while investigations are ongoing. The SDT feels that a mandatory timeframe would interfere with investigations in cases such as these.

Two commenters recommended that the measures should be limited to response actions for detected malware and remove other bullets. In response the SDT agrees and has removed the example measures that were more focused on specific technologies.

One commenter stated that in the guidelines it discusses ‘non-changeable software’ and asks if this is in conflict with definition of Cyber Asset. In response, the SDT believes it is not in conflict. Cyber Asset is a programmable electronic device and devices that are not updateable by the user, but are software or firmware based and do execute a program would still be classified as Cyber Assets.

Requirement Part 3.3

There were many comments that Medium impact locations with no remote connectivity need more than 35 days for signature updates or should not be in scope. Some commented that 35 days is too long for malware updates and it should be shortened. In response, the SDT agrees with both positions and realizes that specifying a time frame on a requirement such as this often means picking a timeframe that is usually not long enough for all of the more extreme cases while at the same time is too long for most ‘normal’ cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order 706 did not direct such a modification and the SDT is more concerned about preventing the unintended consequences of this timeframe and their resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade’s worth of viruses because they may not be able to get last month’s signatures on in 35 days. The SDT believes its in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an ‘arbitrary’ timeframe that satisfies no one.

One commenter stated that 35 days is too long for malware updates and should be shortened. In response, the SDT agrees with both positions and realizes that specifying a timeframe on a requirement such as this often means picking a timeframe that is usually not long enough for all the more extreme cases while at the same time is too long for most 'normal' cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order No. 706 did not direct such a modification and the SDT is more concerned with the unintended consequences of this timeframe and the resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade's worth of viruses because they may not be able to get last month's signatures on in 35 days. The SDT believes it is in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an 'arbitrary' timeframe that satisfies no one.

Several commenters wrote that the requirement is not as clear as the change rationale and the requirement could be gamed to not install any recent sigs. In response, the SDT agrees and has rewritten the requirement for clarity.

A few comments stated that signature updates need to be staged to avoid a large impact of false positives. The included guidance should address this as well. In response, the SDT agrees and has reverted the language back to its V1-V4 state that did include a process for testing and installing the signature updates.

Some commenters questioned that if an entity does not use signature based tools, if they still have a process to update the signatures per the overall requirement. In response, the SDT notes the specific sub requirement is conditional and only applies to "for those methods identified in requirement part 3.1 that use signatures or patterns…" and therefore if an entity has no such methods, the requirement does not apply.

One commenter recommended that the word "available" should be changed to "applicable". In response, the SDT has rewritten the requirement for clarity and to address this and several other comments.

A commenter suggested that the requirement should allow for other anomaly or heuristics based analysis/detection, not just signature updates. In response, Requirement R3.1 allows for any method to be used so that the requirement does not preclude the use of any technology or tool as they constantly improve to keep up with the threats. Requirement R3.3 in particular is only applicable when an entity chooses to use a signature or pattern based tool in order to keep them updated in a timely manner; it does not require their use.

One commenter asked for clarity on what TFEs are allowed for equipment that doesn't run malicious code tools. In response, the SDT notes the requirement has been written at a much higher level than previous versions. The included guidance has numerous suggested methods up to and including policy level measures. Therefore, the SDT feels that TFEs are no longer an issue as the requirement no longer prescriptively requires a single technology tool for addressing the issue.

Requirement R4 General Comments

There were several comments that the rationale language should change 'immediate' detection to 'real time detection' to be consistent with 4.2. In response, the SDT received numerous comments that pointed out issues with the term 'real time' and has deleted it, as well as removing 'immediate' in the rationale.

There was a comment seeking clarity as to whether log events are required for local, remote, or both types of access. In response, the SDT notes that the requirement applies to both High and Medium impact BES Cyber Systems as well as all associated EACMs. The EACMs will include the EAPs for the associated perimeters. Therefore the logging is for both; local access at the BES Cyber Systems themselves, and remote access through the EAP.

One commenter suggested that the guidance include NIST 800-137 as a resource. In response, the SDT agrees and has added the reference to the guidance.

Requirement Part 4.1

Many commenters recommended that the requirement should add the phrase "per device capability". In response, the SDT agrees and has added this concept to the language.

Numerous commenters asked that it be clarified that devices that cannot log do not require a TFE. In response, the SDT has added device capability condition statements to the requirement such that the requirement does not apply if the device does not log the events. In addition, the bulleted list of logged events includes the qualifier 'detected' so that if a device cannot detect such events, then there is nothing to log.

There were several suggestions that 'where technically feasible' should be added to all. In response, the SDT's intent is that the requirement is worded so that what is required matches the device's capability and no more and avoids the use of TFE's due to prescriptive requirements that assume technical capabilities of large classes of Cyber Assets.

Tucson, and SME List commented that TFE should be applied to the logging, not the alerting in 4.2 and suggest removing the TFE in 4.2. In response, the SDT has changed both 4.1 and 4.2 to include the 'per device capability' concept rather than allowing TFE's.

Multiple commenters suggested said that the applicability should change to Medium Impact with ERC. In response, the SDT notes that logging should be enabled wherever it is available. If an isolated or standalone BES Cyber Asset is compromised, then the logs on that device may be the only data the entity will have to investigate the incident.

One commenter suggested that the measures should include samples of logs showing the events are being logged. In response, the SDT agrees and has added the additional example measure.

One commenter suggested that the requirement implies 100% availability of the logging system and suggests adding the 99.9% availability. In response, the SDT notes the comments where the 99.9% was added in CIP-006 pointed out numerous issues with that approach. The SDT believes that the inclusion of Requirement R4.3 states that 100% availability is not required and handles the issue by requiring the entity to have processes in place to respond to outages in a timely manner.

Several commenters sought clarity as to log failed access attempts when deny by default means offending packets are dropped such that there is nothing to log. In response, the SDT notes that a denied access attempt is a failed access attempt.

There were several commenters who suggested that 'malicious software' should be changed to 'malicious code' to be consistent with Requirement R3. In response, the SDT agrees and has made the change.

Many commenters recommended dropping the requirement since its determined after the fact, requires knowledge of intent, and it's not possible to produce a log of 'malicious activity'. In response, the SDT agrees and has removed the sub requirement.

Several commented stated that 4.1.4 is too vague and needs more guidance as to what activities beyond 4.1.1 to 4.1.3 would be included. In response, the SDT agrees and has removed the sub requirement.

One commenter stated that malicious activity should be detected and logged ‘as required in the cyber security incident response plan’. In response, the SDT notes that based on several other industry comments, this sub requirement has been removed.

Requirement Part 4.2

Several commenter stated that ‘real time’ is not the appropriate phrase and some suggested changing to “Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary.” In response, the SDT agrees and has deleted the ‘real time’ phrase.

Also, others commented that ‘real time’ should change to 15 minutes and add ‘where the BES Cyber System is capable.’ In response, the SDT agrees and has deleted the ‘real time’ phrase and the ‘per Cyber Asset or BES System capability’ has been added.

A few commenters recommended that ‘within the BCS capabilities’ be added. In response, the SDT agrees and has added the appropriate phrase.

One commenter stated that a minimum expected set of security events for which alerts should be issued should be prescribed (if the Cyber Asset is capable of detecting and logging those types of events). Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. They also commented that the guidance includes alerts to a display that may not be monitored. In response, the SDT notes that detected malicious code is included, as is detected event logging failure. The SDT agrees that unsuccessful login attempt threshold should be added as it is a requirement in CIP-007 R5.7 and has made this addition. The SDT notes that account lockout is a subset (or post action) of unsuccessful login attempt threshold and has not included it.

There was a comment that the requirement should only apply to Associated Protected Cyber Assets with ERC. In response, the SDT believes that if the BES Cyber Systems have External Routable Connectivity that the associated PCAs will also have that connectivity. In the envisioned rare instance where this is not the case, the requirement allows for the entity to do what is within the device’s capability and no more.

One respondent commented that we need a requirement that trained and knowledgeable people perform the event monitoring activity. In response, the SDT agrees that this is certainly reasonable, but disagrees that it should be an auditable requirement as it raises too many audit issues, such as what do the terms ‘trained’ and ‘knowledgeable’ mean and what is sufficient for each?

A commenter questioned is an alert required for malicious activity if it is automatically quarantined? In response, the SDT notes that alerts are required for detection of malicious code regardless of any subsequent mitigation actions taken. The SDT believes that if malicious code gets through the layers of defense and makes it way on to a BES Cyber System, that is an event that needs the entity’s timely attention and response so the defenses can be shored up for the zero-day that is not detected and quarantined.

One commenter wrote that it was unclear as to whether ‘detected failure’ refers to logging a failure of some event or failure of logging. In response, the SDT has added a clarification that it is failure of the requirement part 4.1 event logging. This would include the failure of the applicable systems logging capability.

There was a recommendation that the measures should include examples of alerts issued. In response, the SDT agrees and has added this as one of the example measures.

Multiple comments suggested that 4.2.1 should change to ‘detected cyber security event’ since not all events are necessarily malicious. In response, the SDT agrees and has changed this part to refer to detected malicious code rather than malicious activity.

There were numerous comments suggesting to change the wording in 4.2.1 to ‘detected events per 4.1’. In response, the SDT agrees and has added the reference to 4.1 for clarity.

One commenter stated that the guidance implies that only technical means are allowed, but requirement does not preclude procedural controls. In response, the SDT notes that the requirement language is the ruling language and guidance is not auditable and is provided to provide further context or examples or assistance in how entities may want to approach meeting the requirement.

Requirement Part 4.3

There were a multitude of commenters who recommended that the requirement add the phrase “human detected event logging failure” to clarify when the clock starts. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

One commenter suggested that ‘after notification’ should be added after ‘next calendar day’. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

A few respondents commented that the requirement should be struck or change the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” In response, the SDT agrees and has struck the requirement.

A few commenters stated that the next calendar day is not enough time to rectify issues. In response, the SDT notes the timeframe is to ‘activate’ a response, not to resolve the issue. The SDT has chosen this in recognition that depending on what caused the failure, there may be widely varying timeframes to resolve the issue. Therefore, the requirement is for timely initiation of a response.

One commenter noted that the requirement presumes but does not prescribe a mechanism for monitoring for logging system failures. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a ‘non-zero defect’ way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenter responded that the timeframe is too short due to distances or other operational situations. There was also a suggestion is to include ‘next business day’. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a ‘non-zero defect’ way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There was one comment that this should only apply to Cyber Assets with ERC. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a ‘non-zero defect’ way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenters recommended that outage handling should be standardized with CIP-006. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There were several comments that the measure should change the word 'attestation' to 'documentation'. In response, the SDT agrees and has made the change.

One comment suggested that the measure should change 'events' to 'failures' to better align with the requirement. In response, the SDT agrees and has made the change.

Requirement Part 4.4

There was a comment that the requirement should change to "Retain BES Cyber System and BES Cyber Asset". In response, the SDT agrees with the concept that the applicability in the requirement did not match the applicability column and has removed the applicability from the requirement by replacing 'BES Cyber System' with 'applicable'.

There were several comments that the TFE language should be struck and add 'within the BCS capabilities." In response, the SDT notes that this requirement is scoped to Control Center environments where the highest degree of logging is required and has the highest degree of more capable Cyber Assets. The SDT feels that in this environment, the industry really should push for 90 days of log retention on these systems.

One commenter suggested that this should apply to all Medium's that can store logs, not just those at control centers. In response, the SDT notes that with the vastly increased numbers and types of field devices that Version 5 will bring into scope, most of which are legacy devices, that putting a mandatory requirement in place that prescribes the length of log retention is not warranted and would cause numerous TFE's.

One commenter wrote that 'identified in 4.1' should be the main qualification for log retention and delete the 'security related' portion for clarity. In response, the SDT agrees and has removed the phrasing.

Some commenters stated that this is in conflict with evidence retention section. Auditors expect to ask for any day's logs in past three years. In response, the SDT has added guidance around this topic. The requirement that is to be audited is that applicable cyber assets maintain 90 days of logs. The compliance evidence requirement is that the entity be able to show that for the historical compliance period, the applicable cyber systems maintained 90 days of logs. The guidance speaks of records of disposition of logs after their 90 days is up.

BPA commented that a media hardware failure that results in loss of stored logs is still a violation. In response, the SDT agrees and has added “except under CIP Exceptional Circumstances” to the requirement as it includes hardware failure.

One commenter stated that this should allow for a timeframe as determined by the Responsible Entity. In response, the SDT notes that 90 days has been the precedent through the previous CIP versions and having no bound means that zero days is valid if determined by the entity. The SDT believes that 90 days is a sufficient lower bound for Control Center environments and has no justification for lowering it in the highest risk environments.

A commenter suggested that the applicability should apply to medium impact with ERC. In response, the SDT notes that this applies to Control Centers. Throughout the history of the CIP standards, all cyber assets in a Control Center are in scope regardless of external connectivity. The SDT believes there is insufficient justification to lower the standard on this point.

One commenter implied that measure 2 requests info about log data that is not in the requirement. Measures 1 and 3 cover the requirement. In response, the SDT agrees and has moved this to the guidance section with a more detailed explanation of the difference between the requirement’s retention period for security purposes and the overall standard’s requirement for compliance measurement purposes.

Requirement Part 4.5

Many responders commented that clarity around who determines the appropriate sampling should be added by including ‘sampling as deemed appropriate by the Responsible Entity’. In response, the SDT agrees and has made the change.

Several commenters noted that the applicability should be ‘High impact including associated PCA’ to clarify logging reviews aren’t at the device level and should exclude EACM/PACMs. In response, the SDT agrees and has modified the applicability, however EACMs should be included. Since Electronic Access Points to ESP’s are EACMs, this is one of the primary logs that should be reviewed.

Several commenters expressed concern that this needs some minimum expectations for logged event review. In response, the SDT notes the intent is included in the requirement which is to identify undetected security incidents. The FERC Order in paragraphs 525 and 628 states, “However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Furthermore, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs.” The SDT believes the intent is that entities manually review logs to insure that automated tools are tuned and alerting on real incidents. The SDT does not believe it should get more prescriptive with the requirement.

There were several commenters who noted that the requirement should change to “Document and implement a secondary control(s), and an associated interval, not to exceed two weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1.” In response, the SDT notes that the FERC Order 706 in paragraphs 525 and 628 are explicit about a manual review. Also, the events identified in 4.1 are requirements so identifying events in 4.5 that should have been caught in 4.1 is a violation. The intent is for the entity to review the logs to see if there are events happening (other than those in 4.1) that the entity should be alerting on. In essence, this is a ‘tuning’ requirement to insure that an entity’s automated Security Information and Event Management (SIEM) type tools are not missing conditions that are appearing in the logs and going undetected.

One commenter suggested that the requirement should change ‘undetected’ to ‘potential Cyber Security Incidents not previously identified or detected’. In response, the SDT notes that in draft one the language included terms such as “unanticipated” and “potential” and received numerous comments to remove these subjective terms.

There were a number of concerns that two weeks is too short and suggest monthly or two month periodicity. In response, the SDT notes that in paragraph 628 of FERC Order 706 states, “The Commission continues to believe that, in general, logs should be reviewed at least weekly”, but leaves it to the ERO to determine the appropriate timeframe. The SDT believes that bi-weekly is an appropriate timeframe given the Commission’s statement concerning weekly reviews.

There was a comment that the phrase “at a minimum every two weeks” could be misconstrued and suggested to mean “at intervals no greater than 15 days.” In response, the SDT agrees that two weeks is a maximum not a minimum and adopts the suggested change.

There was a suggestion in changing the requirement to read “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.” In response, the SDT agrees with the issue and has reworded the requirement based on this and other comments to utilize ‘intervals no greater than 15 days’ for greater specificity.

One commenter suggested that the timeframe should be determined by the Responsible Entity. In response, the SDT notes that in paragraph 628 of FERC Order 706 the Commission ordered the ERO to determine an appropriate timeframe that is less than the 90 days in the requirements of previous versions while stating that weekly reviews are their recommendation. The SDT sees no justification for how this directive can be met if the timeframe is left completely up to the entity to determine.

There were multiple suggestions that the applicability should only apply when automated processes and alerting are not possible or no managed service provider is utilized. In response, the SDT notes from paragraph 525 of FERC Order 706 that “the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings.” The Commission goes on to order the inclusion of manual review even if automated alerts are employed.

One commenter stated that a SIEM is the only real solution and is too expensive for small entities. In response, the SDT notes the requirement is for a manual review, not an automated review. Paragraph 525 of Order 706 makes it clear that even if automated systems are used, the manual review is still required. The requirement does not require installation of SIEM tools, but requires manual review even if SIEM tools are in use.

Several commenters noted that the phrase “signed and” should be deleted in the measure (also in 4.1 measure). In response, the SDT agrees that a signed approval of the review is not in the requirement and this has been deleted from the measure.

QUESTION B24– CIP-007-5 REQUIREMENT R5:

If you disagree with the changes made to CIP-007-5, Requirement R5 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, some of the key issues expressed by commenters included (1) the applicability to Medium Impact BES Cyber Systems with external routable connectivity, particularly in requirement part 5.1 and (2) the obligation for the CIP Senior Manager to authorize specific account types for BES Cyber Systems. The consideration of comments according to major issues and standard sections follows.

Correcting Deficiencies

One comment stated that this requirement should have a find, fix, track, and report mechanism built in so that entities can fix administrative deficiencies rather than consider them a violation of the requirement. In response, the CIP Version 5 approach to correcting deficiencies is that each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in the specified table. This approach of correcting deficiencies complements the compliance concept of internal controls.

Applicability to Low Impact

One commenter suggested that CIP-007-5 R5 should apply to Low Impact BES Cyber Systems. In response, we note the challenge of applying device-specific mandatory and enforceable requirements to low impact BES Cyber Systems exists in the overwhelming number of BES Cyber Assets. NERC survey results from the 2011 CIP filing indicate 90% of the facilities would be considered low impact, and each of these sites can have a potentially large number of Cyber Assets. As a result, the SDT has taken the approach of applying policy level requirements to BES Cyber Systems with the understanding and expectation that the compliance audit and enforcement of the policies will adapt to the significant increase.

TFE for all Requirement Parts

One commenter suggested adding TFE language for the entire requirement due its technical nature. In response, the SDT has identified requirement parts that intentionally allow for a safe-harbor exception process where equivalent mitigation can be shown. However, in some cases, we do not intend the technical limitations of the device to indicate a violation or need for safe-harbor (e.g. password complexity).

Multifactor Authentication
One commenter questioned if multi-factor authentication can replace password authentication without a TFE. In response, the SDT notes that the said requirement applies to password-only authentication but do not preclude other strong authentication mechanisms.

Procedural Controls
One commenter suggested, with regard to CAN-0017, procedural controls should be explicitly allowed in the requirement. However, the SDT points out that Compliance Application Notices do not carry forward to new versions of the standard. Previous versions require both procedural and technical controls for passwords, but this language is not included in the current draft. It would cause more confusion to explicitly allow procedural controls for each requirement part.

Version 5
One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

Summary of Changes Section
Two commenters noted the summary of changes does not correspond to requirements for shared accounts, and in response the SDT has deleted this section which was held over from previous versions.

Requirement Part 5.1
Several entities commented this requirement part should be limited to medium impact with External Routable Connectivity, and the SDT has made this change. However, this requirement still applies to Medium Impact BES Cyber Systems at Control Centers.

Several commented that user access should be a defined term and security controls for system accounts should also exist. In response, we provide a definition in the guidelines, and we believe this term is well understood. In addition, the SDT has added a qualifier for this to apply to interactive user access. We do not define the same controls for system access due to the widely diverse way this could apply. System accounts do not uniformly apply across all devices and operating systems.

Several entities suggested rewording the phrase “where technically feasible” to “within the capability of the BES Cyber System”. In response, the alternative language would not change the TFE trigger for this requirement. There are several instances in which strict compliance can still be met in the absence of a specific technology mechanism to enforce access. The SDT has provided examples in the rationale box for requirement part 5.1 and improved the requirement language to make this point clear.

One commenter requested clarification that user access does not mean front panel read-outs on a device. In response, the SDT has changed “user access” to “interactive user access”, and the SDT has added a rationale statement further describing the intent of this requirement, in which the SDT has explicitly stated front panel read-outs do not qualify as interactive user access.

One commenter proposed that this requirement should be rephrased to limit to only electronic access. In response, the subject matter of the standard and requirement suffice to make the distinction, and we do not want to limit or confuse the possibility of using properly configured physical access controls to demonstrate compliance with this requirement.

One commenter suggested this apply to accounts and not user access. In response, the SDT has chosen to apply this to interactive user access because there may be instances where you do not want to enforce authentication for read-only access.

One commenter suggested specifying the phrase “applicable cyber assets” to qualify this requirement, but the applicability column already qualifies the requirement.

Requirement Part 5.2

Several entities suggested deleting requirement part 5.2 because it is already covered by the CIP-004-5 requirement to authorize users. In response, this requirement only deals with identifying the use of account types. It has been modified to make the intent clearer. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The requirement part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Several commenters advised removing the CIP Senior Manager as the person authorizing these account types. In response, the SDT chose not to remove this in the previous posting as suggested by our previous response to comments, and the SDT has removed the CIP Senior Manager as the person authorizing the account types in this posting.

One commenter proposed that generic accounts must be specified. In response, the SDT has added examples in the guidance section of this standard. The section added reads: "Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level."

One commenter suggested removing the word "authorized" from this requirement. The SDT has incorporated this suggestion by replacing the word "authorized" with the phrase "identify and inventory".

There was a comment submitted as to whether this requirement restricts the use of the specified account types. In response, identification of the accounts provides the necessary control. We do not specify these accounts must be disabled or removed because they are sometimes necessary for operation. Restricting these based on least privilege or need to know is already covered in CIP-004-5 R6.

One commenter suggested that authorization by "delegate(s)" be substitute for "delegate". However, the SDT has removed the requirement to authorize by CIP Senior Manager based on other commenters.

Requirement Part 5.3

Several comments suggested deleting requirement part 5.3 because it is already covered in CIP-004-5 requirements to authorize access. However, the identification of individuals with access to shared account has the additional objective of mitigating the risk of unauthorized access through shared accounts. This differs from the CIP-004-5 Requirement R6 to authorize access. An entity can authorize access and still not know who has access to a shared account. This would make it difficult to revoke access when it is no longer needed.

Several suggested incorporating the change rationale stating that the phrase "individuals storing, losing or inappropriately sharing a password is not a violation of this requirement." In response, the SDT has added this language to the rationale box for CIP-007-5 R5. The language in this section reads, "The term "authorized" is used in the requirement to make clear that an individual storing, losing or inappropriately sharing a password is not a violation of this requirement."

Multiple commenters suggested adding the word "authorized" as a qualifier for access to correspond to the requirement language, and the SDT has made this change.

One commenter suggested that this requirement does not go far enough to restrict the use of privileged access, particularly when operating software. In response, CIP-004-5 R6 restricts the use of privileged access to only those having a documented business need. We do not specify the individual use of privileged and non-privileged access because this is not auditable for mandatory enforceable requirements. This is a good practice, but if this practice were codified in a standard, any individual not following the policy would impose monetary penalties on an organization.

One commenter suggested that the external routable connectivity qualifier should be removed for this Requirement Part in the applicability to match requirement part 5.2. In response, the requirement parts are unrelated, and the qualifier matches that of CIP-004-5 R6, which requires the authorization for electronic access.

Requirement Part 5.4

Several comments suggested revising this requirement part to address a recent RuggedCom vulnerability where a default password was unique to publicly known attributes of the device. In response, the SDT has removed the requirement exception where the "default password is unique to the device or instance of the application", and specified in the rationale that "pseudo-randomly system generated passwords are not considered default passwords".

Several commenters suggested adding the word "known" as a qualifier to default password to avoid the case where the entity was not aware of an undocumented default password by the vendor. The SDT has made this change.

There were several comments that the measure should change the phrase "new devices are deployed" to "new devices are in production" and one commenter suggested removing the phrase altogether since timeframes are covered in the implementation plan. The SDT has made this change from the word "deployed" to "in production", but the timeframe here does not conflict with the implementation timeframe and provides example, high quality evidence to meet this requirement.

One commenter requested clarification of when the default password should be changed. In response, we do not specify a timeframe (i.e. when cyber assets go into production) which could be misinterpreted. Instead, as with all requirements of CIP-007-5, this requirement must be met when a device becomes one of the applicable systems or assets.

Several commenters suggested removing the term “Cyber Assets” within the requirement to match the applicability of BES Cyber System. In response, the SDT has removed this language in deference to the applicability column.

One commenter requested clarification that default password that are unchanged would require changing according to R5.6. In response, this may be the case for interactive user accounts, but this is not necessary to state in the requirement. Changing default passwords meets a different objective to prevent unauthorized access from known credentials.

One commenter suggested excepting when a password is unique to the device. However, many commenters point out that doing so would allow for vulnerabilities where the uniqueness of the device where publicly known (i.e. MAC address).

Requirement Part 5.5

Several commenters suggested modifying the measure for requirement part 5.5 and requirement part 5.6 to better describe the attestation. Another commenter suggested replacing attestations with the ability to present a procedure. Others noted that it is not possible to obtain attestation from unionized workers and suggested adding a separate requirement to use training as a procedural control in place of attestations. In response, the SDT has used provided language to better describe the attestation evidence. The suggestion to use presentation of a procedure as a replacement cannot be used as evidence of implementing a procedure. The suggestion to have a further requirement for training is already covered in the training program specified in CIP-004-5.

One commenter stated that password complexity should be enforced to the maximum extent technically possible. In response, the SDT noted such a policy would create situations where users must write down passwords to remember them. The maximum extent could be exorbitant in some cases.

One commenter also stated that the guidelines state this requirement part is for password-only authentication, but the requirement does not include the same stipulation. BPA and Salt River Project made similar comments to distinguish the case where a PIN is used for multi-factor authentication. In response, the SDT has changed “password-based” to “password-only” in both requirement part 5.5 and 5.6.

Several commenters suggested using verbiage for requirement part 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” In response, although the proposed verbiage is cleaner, it becomes less clear once we specify “system” and the number of characters in the proposal. The SDT therefore decided to continue with the currently drafted language.

One commenter questioned if this new requirement will remove CAN-0017. In response, CANs do not apply to future versions of the standard, and the SDT has explicitly addressed the issue raised by CAN-0017 that either technical or procedural mechanisms can meet the requirement.

One commenter stated that it does not agree with the proscription of password requirements. In response, the SDT has included more prescriptive password requirements in response to a large number of industry comments against having added flexibility. However, the SDT has also attempted to remove some of the problematic provisions of the current version of password requirements that would allow entities to have stronger password policies.

One commenter suggested that the password complexity in requirement part 5.5.2 should specify or define the word “type”. In response, the examples provided in the requirement suffice for specifying password character types. The SDT believes these terms are well-understood by industry and do not necessitate further definitions.

Requirement Part 5.6

Several commenters pointed out the guidance, particularly the recommended password length table, has not updated to reflect the requirement. In response, the SDT has deleted sections of the guidance which no longer have relevance to the requirement.

Several commenters suggested adding a technical feasibility clause to this requirement part because some devices do not allow this capability. In response, the SDT notes that this only applies to user access, and the SDT has modified the requirement part to clarify this. The language as the end of this requirement part reads, “…at least once each calendar year, not to exceed 15 calendar months between changes, where technically feasible.”

One commenter suggested this requirement part explicitly apply to interactive user access, and the SDT has modified this requirement part to address the concern. The beginning of this requirement part reads, “For password-only authentication for interactive user access, either technically or procedurally enforce password changes…”

One commenter suggested adding the language "unless it impacts operation of the BES" to this requirement part. In response, the SDT has added the phrase "where technically feasible" to address these type of exceptions.

One commenter suggested the applicability of 5.6 be modified to match other requirement parts in CIP-007-5 R5. In response, the applicability to those Medium Impact BES Cyber Systems with External Routable Connectivity is due to the periodic nature of this requirement, which may only be feasible on large systems by having such connectivity. The commenter also suggested periodically is misspelled periodicity, but the SDT intends the latter as this is an attribute of the policy instead of a modifier.

One commenter suggested incorporating the language in the guidance table to include periodicity provisions for plant outages and disabled accounts. In response, for disabled accounts, a password change is not required because these do not qualify as providing interactive user authentication. The requirement does not have provisions for plant outages due to the widely varying schedules for plant outages. The SDT also notes that this requirement applies to those Medium Impact BES Cyber Systems with External Routable Connectivity.

A commenter proposed having a password change every 15 months. The SDT has incorporated this suggestion as part of an overall modification of annual periodic requirements in the CIP standards.

A commenter proposed to allow the entity to specify a password change periodicity, but the SDT has specified this periodicity based on a large number of comments against having this flexibility.

There was one comment that suggested the password change periodicity should be much shorter (i.e. quarterly). In response, the SDT notes that password change requirements should be considered in context with all of the password requirements, and shorter password change requirements can often result in poor password protection and selection by individuals.

Requirement Part 5.7

Several commenters suggested this requirement has the potential for creating a denial of service vulnerability to lockout all accounts to the system if entities configure all accounts for lockout. The SDT has not included the proposal to specify "user accounts" for limiting login attempts because it is too specific and has the potential to cause confusion. Although the requirement does not prescribe this vulnerability, it does allow for it. Consequently, the SDT has included guidance in avoiding this configuration in the rationale.

Several commenters requested clarification on what the clause “where technically feasible” qualifies for this requirement part. In response, this requirement part has been modified to make clear the TFE triggering language qualifies both options. Furthermore, a TFE would only be necessary based on failure to implement either option.

Several commenters suggested this requirement should be deleted as it was not directed by FERC or otherwise align with the alerting requirements of CIP-007-5 requirement part 4.2. In response, this requirement is part of a more reasonable overall password security standard. As a trade-off to providing more flexibility to password policies, this requirement is highly effective to prevent online password attacks. This does not duplicate CIP-007-5 requirement part 4.2 because this alert is not required to be configured by that requirement.

One commenter requested additional guidance on the threshold for unsuccessful login attempts. The SDT has added this to the guidance section of this standard. Language was added which reads, “The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate.”

Multiple commenters suggested that a minimum threshold parameter for account lockout should be specified. In response, a value is not specified here because this requirement protects against password cracking through online password cracking. Given the additional password policy requirements, the threshold for this setting can be very high, up to 100 or more.

One commenter requested the requirement part make clear these do not apply to Protected Cyber Assets such as printers and multi-function machines. In response, this requirement does apply to Protected Cyber Assets. This is a part of an overall protection against unauthorized access, which would include Protected Cyber Assets that have direct connections with the BES Cyber System.

VRFs

There was one comment that suggested the VRF should be Lower for Medium Impact BES Cyber Systems. In response, the impact level of the BES Cyber System is accounted for by the applicability of CIP-004 through CIP-011 requirements. A violation for a Medium Impact BES Cyber System cannot be considered directly with a High Impact BES Cyber System because they have less application of compensating security requirements.

VSLs

There was one comment that noted the High VSL includes the phrase “use of” where the associated requirement refers to only enablement of generic accounts and that the Severe VSL includes criteria for failure to implement password procedures, which might imply the required use of passwords. The VSL language regarding the enablement of generic account types has been updated to match the requirement. We do not agree the Severe VSL language implies a requirement to only use passwords. The VSLs are only used to describe violations, and use of authentication alternatives to passwords would not be a violation.

One commenter noted the Severe VSL is not consistent with the requirement and the SDT has updated the VSLs to align with modifications to the requirement.

Guideline

There was a recommendation that the guideline section needs to define generic accounts, and the SDT has added this to the guidelines.

Questions with Votes Only:

CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
NESCOR/NESCO	No
ACES Power Marketing	No
Hydro One	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes

Organization	Yes or No
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes

Organization	Yes or No
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
PJM Interconnection	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes

Organization	Yes or No
Utility Services Inc	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No

Organization	Yes or No
LCEC	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Snohomish County PUD	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
San Diego Gas & Electric	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177,	Yes

Organization	Yes or No
JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes

Organization	Yes or No
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." 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
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No
IRC Standards Review Committee	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
NRG Energy Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

4. CIP-004-5 R4 states “Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No
ACES Power Marketing	No
IRC Standards Review	No

Organization	Yes or No
Committee	
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No

Organization	Yes or No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
New York Power Authority	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
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
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes
California ISO	Yes

5. CIP-004-5 R5 states “Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
PSEG	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes

Organization	Yes or No
SPP and Member companies	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity	Yes

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

Organization	Yes or No
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Pepco Holdings Inc & Affiliates	No
SMUD & BANC	No

Organization	Yes or No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
NYISO	No
Farmington Electric Utility System	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service	Yes

Organization	Yes or No
Company	
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
ISO New England Inc.	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
SPP and Member companies	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern Company Services, Inc.	No
Southern California Edison company	No

Organization	Yes or No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
ATCO Electric	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Lakeland Electric	No
Ameren	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
MEAG Power	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Springfield Utility Board	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
PSEG	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes

Organization	Yes or No
Cowlitz County PUD	Yes

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

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

Organization	Yes or No
SPP and Member companies	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy	No

Organization	Yes or No
Company	
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
NRG Energy Companies	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes

Organization	Yes or No
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
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
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

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

Organization	Yes or No
ACES Power Marketing	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Progress Energy	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No

Organization	Yes or No
PSEG	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba	Yes

Organization	Yes or No
National Grid)	
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards	No

Organization	Yes or No
Review Subcommittee	
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service	No

Organization	Yes or No
Company	
Southern Company Services, Inc.	No
Western Area Power Administration	No
Salt River Project	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No

Organization	Yes or No
Lincoln Electric System	No
United illuminating Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
PSEG	No

Organization	Yes or No
San Diego Gas & Electric	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
MEAG Power	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Southern California Edison company	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
The Empire District Electric Company	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
PNM Resources	No
BC Hydro	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity	No

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
Portland General Electric	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its	No

Organization	Yes or No
affiliates	
Deseret Power	No
Los Angeles Department of Water and Power	No
California ISO	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes

16. **CIP-006-5 R3 states “Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.” 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
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
IRC Standards Review Committee	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No

Organization	Yes or No
Texas Reliability Entity	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Los Angeles Department of Water and Power	No
PPL Corporation NERC Registered Affiliates	Yes
Duke Energy	Yes
Dominion	Yes
FirstEnergy	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security	Yes

Organization	Yes or No
Technologies, Inc.	
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

18. **CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its affiliates	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	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
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

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

Organization	Yes or No
Hydro One	No
Arizona Public Service Company	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Hydro-Quebec TransEnergie	No
LCEC	No
Lincoln Electric System	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Kansas City Power & Light	No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power	Yes

Organization	Yes or No
Agency	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power	Yes

Organization	Yes or No
Cooperative	
US Bureau of Reclamation	Yes
California ISO	Yes

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." 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
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SPP and Member companies	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes

Organization	Yes or No
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Western Area Power Administration	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No

Organization	Yes or No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No

Organization	Yes or No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
NYISO	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
United illuminating Company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Consumers Energy Company	No

Organization	Yes or No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc (NCR01177, JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
ATCO Electric	Yes
LCEC	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
PSEG	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT